

Lesley E. Weaver (SBN 191305)
BLEICHMAR FONTI & AULD LLP
555 12th Street, Suite 1600
Oakland, CA 94607
Tel.: (415) 445-4003
Fax: (415) 445-4020
lweaver@bfalaw.com

Derek W. Loeser (admitted *pro hac vice*)
KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101
Tel.: (206) 623-1900
Fax: (206) 623-3384
dloeser@kellerrohrback.com

Plaintiffs' Co-Lead Counsel

Additional counsel listed on signature page

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

IN RE: FACEBOOK, INC. CONSUMER
PRIVACY USER PROFILE LITIGATION

MDL No. 2843
Case No. 18-md-02843-VC

This document relates to:

ALL ACTIONS

**PLAINTIFFS' OPPOSITION TO
MOTION OF DEFENDANT FACEBOOK,
INC. TO DISMISS PLAINTIFFS'
CONSOLIDATED COMPLAINT**

Judge: Hon. Vince Chhabria
Courtroom: 4, 17th Floor
Hearing Date: January 23, 2019
Hearing Time: 10:00 a.m.

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	ARGUMENT	4
A.	Facebook Users Have Article III Standing to Pursue Relief Against Facebook.	4
1.	Plaintiffs Have Suffered or Face a Substantial Threat of Identity Theft or Fraud.....	5
2.	Plaintiffs Have Suffered a Cognizable Injury to Their Privacy Interests.....	7
3.	Plaintiffs Have Suffered Injury to Their Property Interests.....	8
B.	Plaintiffs Did Not Consent to Facebook’s Disclosure of Personal Information...	10
1.	Users Did Not Consent to the Privacy and Data Use Policies When They Opened a Facebook Account.	10
2.	Users Did Not Consent to the Privacy and Data Use Policies Through the SRR.	12
3.	The Privacy and Data Use Policies Did Not Disclose Third-Party Access to Their Content and Information Through Their Friends.....	14
4.	The Language Facebook Claims Disclosed and Obtained Consent Was Contradicted in the User Experience by the Privacy Settings.....	16
C.	Facebook Cannot Hide Behind an Exculpatory Clause.	18
D.	Facebook Violated Federal Statutes.....	20
1.	Plaintiffs Have Standing to Bring VPPA and SCA Claims.....	20
2.	Facebook Violated the VPPA.	20
3.	Facebook Violated the Stored Communications Act.	22
E.	Plaintiffs’ Privacy Claims Should Be Upheld.	24
1.	Facebook’s General Challenges to Plaintiffs’ Privacy Claims Are Unavailing.....	24
2.	Plaintiffs State a Claim for Public Disclosure of Private Facts.	27

3.	Facebook Violated Plaintiffs’ Right of Publicity.....	27
F.	Plaintiffs State a Claim for Fraudulent Omission.....	28
G.	Facebook Violated the Unfair Competition Law.....	31
1.	Plaintiffs Have Standing to Assert UCL Claims.....	31
2.	Plaintiffs State a UCL Claim Under the “Unlawful” Prong.....	31
3.	Plaintiffs State a UCL Claim Under the “Fraudulent” Prong.....	31
4.	Plaintiffs State a UCL Claim Under the “Unfair” Prong.....	32
5.	Plaintiffs Plead Entitlement to UCL Restitution.....	32
H.	Facebook Was Unjustly Enriched Through Its Sale of Access to Plaintiffs’ Content and Information.....	33
1.	This Claim Is Not Barred by Facebook’s Agreement with Users.....	34
2.	Restitution Is the Appropriate Remedy in Quasi-Contract.....	35
I.	Plaintiffs State a Claim for Negligence and Gross Negligence.....	36
J.	In the Alternative to Quasi-Contract, Facebook Breached the Terms of the SRR With Users.....	39
1.	Plaintiffs Have Standing to Pursue a Breach of Contract Claim.....	39
2.	Facebook Breached Its Promise Not to Share Content and Information With Third Parties.....	39
3.	Plaintiffs Have Suffered Damages.....	41
K.	Facebook Breached Its Implied Covenant of Good Faith and Fair Dealing with Users.....	41
L.	All of Plaintiffs’ Claims Are Timely.....	41
M.	Plaintiffs’ Non-California Claims Should Be Dismissed Without Prejudice.....	43
III.	IN THE ALTERNATIVE, PLAINTIFFS SEEK LEAVE TO AMEND.....	44
IV.	CONCLUSION.....	44

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>A & M Produce Co. v. FMC Corp.</i> , 135 Cal. App. 3d 473 (1982)	19
<i>In re Adobe Sys., Inc. Privacy Litig.</i> , 66 F. Supp. 3d 1197 (N.D. Cal. 2014).....	32
<i>Aerojet-Gen. Corp. v. Transport Indem. Co.</i> , 17 Cal. 4th 38 (1997).....	34
<i>Aguilera v. Pirelli Armstrong Tire Corp.</i> , 223 F.3d 1010 (9th Cir. 2000)	10, 39
<i>Amazon.com v. Lay</i> , 758 F. Supp. 2d 1154 (W.D. Wash. 2010)	21
<i>Amtower v. Photon Dynamics, Inc.</i> , 158 Cal. App. 4th 1582 (2008)	13
<i>In re Anthem, Inc. Data Breach Litig.</i> , 162 F. Supp. 3d 953 (N.D. Cal. 2016).....	31, 32
<i>In re Anthem, Inc. Data Breach Litig.</i> , 2016 WL 3029783 (N.D. Cal. May 27, 2016)	9, 10, 31, 32
<i>Antman v. Uber Technologies, Inc.</i> , 2015 WL 6123054 (N.D. Cal. Oct. 19, 2015)	7
<i>Astiana v. Hain Celestial Grp., Inc.</i> , 783 F.3d 753 (9th Cir. 2015)	35
<i>Attias v. Carefirst, Inc.</i> , 865 F.3d 620 (D.C. Cir. 2017)	6
<i>Avery v. Integrated Healthcare Holdings, Inc.</i> , 218 Cal. App. 4th 50 (2013)	12
<i>Bailey v. United States</i> , 289 F. Supp. 2d 1197 (D. Haw. 2003)	18
<i>Beacon Residential Cmty. Ass’n v. Skidmore, Owings & Merrill LLP</i> , 59 Cal. 4th 568 (2014).....	37

<i>Berkson v. Gogo LLC</i> , 97 F. Supp. 3d 359 (E.D.N.Y. 2015).....	11
<i>Bertino & Assocs., Inc. v. R L Young, Inc.</i> , 2013 WL 3949028 (D.N.J. Aug. 1, 2013)	34
<i>Birdsong v. Apple, Inc.</i> , 590 F.3d 955 (9th Cir. 2009)	9
<i>Byars v. SCME Mortg. Bankers, Inc.</i> , 109 Cal. App. 4th 1134 (2003)	32
<i>Cabral v. Ralphs Grocery Co.</i> , 51 Cal. 4th 764 (2011).....	37
<i>Campbell v. Facebook Inc.</i> , 77 F. Supp. 3d 836 (N.D. Cal. 2014).....	14, 16
<i>In re Carrier IQ, Inc.</i> , 78 F. Supp. 3d 1051 (N.D. Cal. 2015).....	30
<i>Cel-Tech Commc’n, Inc. v. L.A. Cellular Tel. Co.</i> , 20 Cal. 4th 163 (1999).....	32
<i>Centinela Freeman Emergency Med. Assocs. v. Health Net of Cal., Inc.</i> , 1 Cal. 5th 994, 1015 (2016)	36, 37
<i>Chan v. Drexel Burnham Lambert, Inc.</i> , 178 Cal. App. 3d 632 (1986)	14
<i>Circle Click Media LLC v. Regus Mgt. Grp. LLC</i> , 2013 WL 57861 (N.D. Cal. Jan. 3, 2013).....	34
<i>City of Santa Barbara v. Superior Court</i> , 41 Cal. 4th 747 (2007).....	18
<i>Clapper v. Amnesty Int’l USA</i> , 568 U.S. 398 (2013).....	5
<i>Cohen v. Facebook, Inc.</i> , 798 F. Supp. 2d 1090 (N.D. Cal. 2011).....	15, 16
<i>Corona v. Sony Pictures Entm’t, Inc.</i> , 2015 WL 3916744 (N.D. Cal. June 15, 2015).....	10, 31
<i>In re: Countrywide Fin. Corp. Mortg. Mktg. & Sales Practices Litig.</i> , 601 F. Supp. 2d 1201 (S.D. Cal. 2009)	34

<i>Cty. of Contra Costa v. Kaiser Found. Health Plan, Inc.</i> , 47 Cal. App. 4th 237 (1996)	16, 40
<i>Davidson v. City of Westminster</i> , 32 Cal. 3d 197 (1982)	29
<i>In re De Laurentiis Entm't Grp.</i> , 963 F.2d 1269 (9th Cir. 1992)	35
<i>Dora v. Frontline Video, Inc.</i> , 15 Cal. App. 4th 536 (1993)	28
<i>Durell v. Sharp Healthcare</i> , 183 Cal. App. 4th 1350 (2010)	32
<i>Eastwood v. Superior Court</i> , 149 Cal. App. 3d 409 (1983)	28
<i>Ehling v. Monmouth-Ocean Hosp. Serv. Corp.</i> , 961 F. Supp. 2d 659 (D.N.J. 2013)	17, 23
<i>Eichenberger v. ESPN, Inc.</i> , 876 F.3d 979 (9th Cir. 2017)	20, 21
<i>Eidson v. Medtronic, Inc.</i> , 40 F. Supp. 3d 1202 (N.D. Cal. 2014)	42
<i>Ellis v. J.P. Morgan Chase & Co.</i> , 950 F. Supp. 2d 1062 (N.D. Cal. 2013)	34
<i>In re Facebook Biometric Info. Privacy Litig.</i> , 185 F. Supp. 3d 1155 (N.D. Cal. 2016)	12
<i>In re Facebook PPC Advert. Litig.</i> , 2010 WL 3341062 (N.D. Cal. Aug. 25, 2010)	18
<i>In re Facebook Privacy Litig.</i> , 192 F. Supp. 3d 1053 (N.D. Cal. 2016)	39
<i>Facebook, Inc. v. Superior Court</i> , 15 Cal. App. 5th 729 (2017)	25
<i>Folgelstrom v. Lamps Plus, Inc.</i> , 195 Cal. App. 4th 986 (2011)	26
<i>Fox v. Ethicon Endo-Surgery, Inc.</i> , 35 Cal. 4th 797 (2005)	43

<i>Fraley v. Facebook, Inc.</i> , 830 F. Supp. 2d 785 (N.D. Cal. 2011).....	14, 41
<i>Frangipani v. Boecker</i> , 64 Cal. App. 4th 860 (1998)	10
<i>Fteja v. Facebook, Inc.</i> , 841 F. Supp. 2d 829 (S.D.N.Y. 2012).....	12
<i>Gardner v. Downtown Porsche Audi</i> , 180 Cal. App. 3d 713 (1986)	19
<i>Gonzalez v. Cent. Elec. Coop.</i> , 2009 WL 3415235 (D. Or. Oct. 15, 2009).....	21
<i>Goodman v. HTC Am., Inc.</i> , 2012 WL 2412070 (W.D. Wash. June 26, 2012).....	7, 26
<i>In re Google Android Consumer Privacy Litig.</i> , 2013 WL 1283236 (N.D. Cal. Mar. 26, 2013).....	9
<i>In re Google Android Consumer Privacy Litig.</i> , 2014 WL 988889 (N.D. Cal. Mar. 10, 2014).....	33
<i>In re Google Inc. Cookie Placement Consumer Privacy Litig.</i> , 806 F.3d 125 (3d Cir. 2015)	7, 26
<i>In re: Google Inc. Gmail Litig.</i> , 2014 WL 1102660 (N.D. Cal. Mar. 18, 2014).....	14
<i>In re Google, Inc. Privacy Policy Litig.</i> , 2013 WL 6248499 (N.D. Cal. Dec. 3, 2013).....	9
<i>Greystone Homes, Inc. v. Midtec, Inc.</i> , 168 Cal. App. 4th 1194 (2008)	38
<i>Hernandez v. Hillsides, Inc.</i> , 47 Cal. 4th 272 (2009).....	25
<i>Hill v. NCAA</i> , 7 Cal. 4th 1 (1994).....	25, 26
<i>Hinojos v. Kohl's Corp.</i> , 718 F.3d 1098 (9th Cir. 2013)	41
<i>Hughey v. Drummond</i> , 2015 WL 4395013 (E.D. Cal. July 16, 2015).....	24

<i>In re Hulu Privacy Litig.</i> , 2012 WL 3282960 (N.D. Cal. Aug. 10, 2012)	20, 21
<i>In re Hulu Privacy Litig.</i> , 2014 WL 1724344 (N.D. Cal. Apr. 28, 2014)	21, 22
<i>In re Hulu Privacy Litig.</i> , 2014 WL 2758598 (N.D. Cal. June 17, 2014)	22
<i>In re iPhone Application Litig.</i> , 2011 WL 4403963 (N.D. Cal. Sept. 20, 2011)	9
<i>In re iPhone Application Litig.</i> , 844 F. Supp. 2d 1040 (N.D. Cal. 2012)	17, 20, 32
<i>J'Aire Corp. v. Gregory</i> , 24 Cal. 3d 799 (1979)	36, 37, 38
<i>Jolly v. Eli Lilly & Co.</i> , 44 Cal. 3d 1103 (1988)	43
<i>Kinsey v. Macur</i> , 107 Cal. App. 3d 265 (1980)	27
<i>KNB Enters. v. Matthews</i> , 78 Cal. App. 4th 362 (2000)	27
<i>Korea Supply Co. v. Lockheed Martin</i> , 29 Cal. 4th 1134 (2003)	33
<i>Krottner v. Starbucks Corp.</i> , 628 F.3d 1139 (9th Cir. 2010)	6
<i>Kwikset Corp. v. Superior Court</i> , 51 Cal. 4th 310 (2011)	33
<i>LaCourt v. Specific Media, Inc.</i> , 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011)	7
<i>In re: Lenovo Adware Litig.</i> , 2016 WL 6277245 (N.D. Cal., Oct. 27, 2016)	38
<i>Lewis v. Casey</i> , 518 U.S. 343 (1996)	9
<i>Lhotka v. Geographic Expeditions, Inc.</i> , 181 Cal. App. 4th 816 (2010)	20

<i>Lierboe v. State Farm Mut. Auto. Ins. Co.</i> , 350 F.3d 1018 (9th Cir. 2003)	9
<i>In re LinkedIn User Privacy Litig.</i> , 932 F. Supp. 2d 1089 (N.D. Cal. 2013).....	38
<i>Long v. Provide Commerce, Inc.</i> , 245 Cal. App. 4th 855 (2016)	10
<i>Lopez v. Smith</i> , 203 F.3d 1122 (9th Cir. 2000)	44
<i>Low v. LinkedIn Corp.</i> , 2011 WL 5509848 (N.D. Cal. Nov. 11, 2011)	7
<i>Lujan v. Defenders of Wildlife</i> , 504 U.S. 555 (1992)	5, 9
<i>Matera v. Google Inc.</i> , 2016 WL 5339806 (N.D. Cal. Sept. 23, 2016)	10, 16, 23
<i>Merck & Co. v. Reynolds</i> , 559 U.S. 633 (2010)	43
<i>Miller v. Nat’l Broad. Co.</i> , 187 Cal. App. 3d 1463 (1986)	25
<i>Moeller v. Am. Media, Inc.</i> , 235 F. Supp. 3d 868 (E.D. Mich. 2017)	35
<i>Nguyen v. Barnes & Noble, Inc.</i> , 763 F.3d 1171 (9th Cir. 2014)	12
<i>Nicosia v. Amazon.com, Inc.</i> , 834 F.3d 220 (9th Cir. 2016)	11
<i>Norcia v. Samsung Telecomms. Am.</i> , 845 F.3d 1279 (9th Cir. 2017)	12, 13
<i>Opperman v. Path, Inc.</i> , 205 F. Supp. 3d 1064 (N.D. Cal. 2016).....	14, 25
<i>Ott v. Alfa-Laval Agri, Inc.</i> , 31 Cal. App. 4th 1439 (1995)	38
<i>Patel v. Facebook Inc.</i> , 290 F. Supp. 3d 948 (N.D. Cal. 2018).....	39

<i>Pelletier v. Alameda Yacht Harbor</i> , 188 Cal. App. 3d 1551 (1986)	19
<i>Platte Anchor Bolt, Inc. v. IHI, Inc.</i> , 352 F. Supp. 2d 1048 (N.D. Cal. 2004).....	38
<i>Precision Pay Phones v. Qwest Commc'ns Corp.</i> , 210 F. Supp. 2d 1106 (N.D. Cal. 2002).....	33
<i>Raisin Bargaining Ass'n v. Hartford Cas. Ins. Co.</i> , 2010 WL 3783871 (E.D. Cal. Sept. 27, 2010).....	34
<i>Ruiz v. Gap, Inc.</i> , 622 F. Supp. 2d 908 (N.D. Cal. 2009).....	10
<i>Shaw v. Regents of University of California</i> , 58 Cal. App. 4th 44 (1997)	13
<i>ShopKo Stores Operating Co. v. Balboa Capital Corp.</i> , 2017 WL 3579879 (C.D. Cal. July 13, 2017).....	43
<i>Silha v. ACT, Inc.</i> , 807 F.3d 169 (7th Cir. 2015)	9
<i>In re Sony Gaming Networks and Customer Data Sec. Breach Litigation</i> , 903 F. Supp. 2d 942 (S.D. Cal. 2012)	31
<i>Spokeo, Inc. v. Robins</i> , 136 S. Ct. 1540 (2016)	5, 20, 39
<i>Stewart v. Electrolux Home Prods., Inc.</i> , 304 F. Supp. 3d 894 (E.D. Cal. 2018)	38
<i>Stitt v. Citibank</i> , 942 F. Supp. 2d 944 (N.D. Cal. 2013).....	34
<i>In re: SuperValu, Inc.</i> , 870 F.3d 763 (8th Cir. 2017)	7
<i>Susan B. Anthony List v. Driehaus</i> , 134 S. Ct. 2334 (2014)	6
<i>Sweet v. Johnson</i> , 169 Cal. App. 2d 630 (1959)	39
<i>Tenet Healthsystem Desert, Inc. v. Blue Cross of Cal.</i> , 245 Cal. App. 4th 821 (2016)	30

<i>Tunkl v. Regents of University of California</i> , 60 Cal. 2d 92 (1963).....	18, 19
<i>Van Patten v. Vertical Fitness Grp., LLC</i> , 847 F.3d 1037 (9th Cir. 2017)	7
<i>In re Vizio, Inc., Consumer Privacy Litig.</i> , 238 F. Supp. 3d 1204 (C.D. Cal. 2017).....	21, 29, 30
<i>Vucinich v. Paine, Webber, Jackson & Curtis, Inc.</i> , 739 F.2d 1434 (9th Cir. 1984)	43
<i>Warth v. Seldin</i> , 422 U.S. 490 (1975)	9
<i>Windsor Mills, Inc. v. Collins & Aikman Corp.</i> , 25 Cal. App. 3d 987 (1972)	12
<i>Wolschlager v. Fid. Nat’l Title Ins. Co.</i> , 111 Cal. App. 4th 784 (2003)	12, 13
<i>Woods v. Google Inc.</i> , 2011 WL 3501403 (N.D. Cal. Aug. 10, 2011)	41
<i>In re Yahoo! Inc. Customer Data Sec. Breach Litig.</i> , 2017 WL 3727318 (N.D. Cal. Aug. 30, 2017)	31, 41
<i>In re Yahoo! Inc. Customer Data Sec. Breach Litig.</i> , 313 F. Supp. 3d 1113 (N.D. Cal. 2018).....	<i>passim</i>
<i>In re Zappos.com, Inc.</i> , 888 F.3d 1020 (9th Cir. 2018)	6

Statutes

15 U.S.C. § 6501, et seq.	19
18 U.S.C. § 2701, et seq.	<i>passim</i>
18 U.S.C. § 2710.....	20, 21, 22, 31
Cal. Bus. & Prof. Code § 17200, et seq.	30, 31, 32, 33
Cal. Civ. Code § 654.....	40
Cal. Civ. Code § 1798.125(b)(1)	8
Cal. Civ. Code § 3360.....	39

California Consumer Privacy Act of 2018	8, 19
Illinois Biometric Information Privacy Act of 2008.....	19

Other Authorities

California Constitution Article I, Section I	24, 26
Restatement (Second) of Torts § 892A (1979).....	19

I. INTRODUCTION

This case seeks to hold Facebook, Inc. (“Facebook”) accountable for distributing users’ private content and information, without their consent, to millions of application (“app”) developers and certain of its business partners, which are some of the world’s largest corporations. Facebook built its social network by encouraging users to share personal information on its platform, promising them that their “privacy is very important to us.” ¶¶ 243-44, 276.¹ However, it has become apparent that it was only the illusion of privacy that Facebook deemed “very important,” because that illusion allowed Facebook to violate its users’ trust and exploit their personal information.

Facebook’s misconduct took two forms. First, unbeknownst to users, Facebook delivered their content and information to its “business partners”—companies as varied as Garmin, Opera Software, Verizon, Amazon, and Huawei—when users used their Facebook log-in to interact with those companies. ¶¶ 169-74, 226, 491, 496, 516, 522, 559, 575. If User A’s friend, User B, logged onto a business partner’s platform—Amazon, for example—using User B’s Facebook account, Amazon would have access to User A’s content and information. ¶¶ 112-14, 170-72. Similarly, if User A’s friend, User B, downloaded an app, that app developer would have access to all content that User A’s friends shared with him, including private photos and private messages. ¶¶ 119, 129, 145-57. Second, Facebook knowingly allowed these third parties to access user content and information, overriding privacy settings, with no controls over how the content was used or limitations on further dissemination—as the Cambridge Analytica LLC (“Cambridge Analytica”) scandal has shown. ¶¶ 4-7, 147, 431.

Thus, Facebook’s illusory privacy settings promised users they could decide who could view the content they shared, including photos, private messages and their “likes.” In reality, beneath Facebook’s network user platform, an entire infrastructure collected user content and

¹ Cites to “¶” refer to the Corrected Consolidated Complaint, ECF No. 152-2.

distributed it to app developers and business partners, even when users had earmarked that content as private. ¶¶ 169-70, 226, 338.

Facebook argues strenuously that users consented to all of these practices. But consent first requires disclosure, and these practices were not disclosed. The operative terms of service—the Statement of Rights and Responsibilities (“SRR”)—did not tell users that through their friends’ behavior Facebook was giving privately shared content to business partners and millions of app developers. ¶¶ 226, 408, 491, 496, 516, 522, 559, 575. Facebook put information about these practices in so-called “Data Policies” to which users never agreed. ¶¶ 213-15, 250-60, 273, 277. In fact, from 2009 through 2012, users were not required to accept *any* terms before entering their name, email address, sex and birthdate, and clicking “sign me up.” ¶¶ 261-64. In any event, there is no disclaimer in any of these documents that clearly and prominently tells users that their private communications with friends are shared with third parties through their friends’ actions. Notably, Facebook’s 2018 Terms of Service, the re-named “SRR,” now contain language that at least addresses the issue, although it is still opaque. *See* Declaration of Lesley E. Weaver in Support of Plaintiffs’ Opposition to Motion of Defendant Facebook, Inc. to Dismiss Plaintiffs’ Consolidated Complaint (“Weaver Declaration”), Exhibit 1.

The exposure of users’ personal information has injured them in multiple ways. For one, it has put them at risk of imminent harm. Some plaintiffs have already experienced attempts to hack into their accounts as well as phishing. ¶ 408. Experts agree that users whose data was stolen are at increased risk of identity theft and financial fraud. And, contrary to Facebook’s arguments, Plaintiffs are not required to have suffered identity theft to have standing.

Unlike data breach cases that involve the theft of a few pieces of personal information, significant amounts of highly personal content were made available by Facebook to these third parties. By allowing users to believe their communications were private, Facebook induced them to reveal more than they would have otherwise, which Facebook then exploited for revenue and benefits. The difference in value between the content that users would have shared in a public forum, and the value of the more intimate information they revealed in a private forum, which

Facebook then monetized, constitutes a piece of Plaintiffs' economic harm. The notion that users' content and information is property that has significant economic value should not be controversial, since it is the very cornerstone of Facebook's business model. Facebook calculates average revenue per user ("ARPU") based specifically on the content it mines from each user, and touts this to investors and its business partners who are seeking to target users based on that information. ¶¶ 359-70. Facebook's \$40 billion in revenue last year was built upon the value of this content. ¶¶ 1-2.

Users have suffered injury, too, by being deprived of the service they reasonably believed they were signing up for. Instead of a forum where some conversations can be private, subject to users' decisions about what to share with whom, they joined a service where there are no truly private conversations. To protect their privacy now, users must either reduce their participation or delete their account, losing the full benefit of their online community. Indeed, following the Cambridge Analytica scandal, many users have left Facebook.²

Users have suffered irreparable, permanent injury to their privacy. Facebook has made users' personal content available to unvetted, unaudited and unscrupulous third parties who now target users with political and other content crafted from assumptions about users' psychological make-up. ¶¶ 360-76. This is not the kind of targeted advertising that a reasonable user would have expected, like receiving ads for football tickets while on a sporting goods store's website. Instead, this "psychographic marketing" is based on personality assessments augmented with content and information derived from users' interactions with friends, which Facebook told users would be private. The targets of this messaging include children between the ages of 13 and 18,

² 44% of young adult users have deleted their Facebook app from their phone in the last year, and roughly half of them have deleted their accounts. Andrew Perrin, *Americans are changing their relationship with Facebook*, Pew Research Center (Sept. 5, 2018), <http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/>.

such as Plaintiff Doe, who will be tied to that content for the rest of their lives. ¶ 45-46.³ The Complaint alleges, and experts agree, that psychographic marketing is harmful and invasive, particularly because the practices have been largely undisclosed to consumers. ¶¶ 13, 368-401. Because electronic information is easily replicable, users cannot remove it from others' possession once taken. Even if users quit Facebook, invasive targeting may follow them forever.⁴ ¶ 416.

These injuries do raise important "policy and social issues," MTD⁵ 3, but they also give rise to cognizable legal claims grounded in the law's time-honored protections for property and privacy. It may be convenient for Facebook to argue that scrutiny by the political branches excludes accountability in the courts, but such an argument has no basis in law.

Even now, Facebook refuses to provide specific information to users that would help users protect themselves against identify theft, financial fraud, manipulation and unwanted messaging. As one prominent journalist has noted, Facebook's tactic, in response to the inquiries triggered by the Cambridge Analytica scandal has been to delay, deny and deflect.⁶ This lawsuit seeks accountability, damages, protection and restitution for users.

For the reasons set forth below, Facebook's motion should be denied in its entirety.

II. ARGUMENT

A. Facebook Users Have Article III Standing to Pursue Relief Against Facebook.

Article III standing exists if the plaintiff has (i) "suffered an injury in fact" that is (ii) caused by "the conduct complained of" and (iii) that "will be redressed by a favorable decision."

³ Kelsey Munro, *China's social credit system 'could interfere in other nations' sovereignty'*, The Guardian (June 27, 2018), https://www.theguardian.com/world/2018/jun/28/chinas-social-credit-system-could-interfere-in-other-nations-sovereignty?CMP=share_btn_link.

⁴ See, e.g., Mark Zuckerberg, *Bringing the World Closer Together*, Facebook, June 22, 2017, <https://www.facebook.com/notes/mark-zuckerberg/bringing-the-world-closer-together/10154944663901634>.

⁵ Mem. of Law in Supp. of Mot. of Def. Facebook, Inc. to Dismiss Pls.' Consolidated Compl. ("Motion to Dismiss" or "MTD"), ECF No. 184-1.

⁶ Sheera Frenkel, et al., *Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis*, N.Y. Times (Nov. 14, 2018), <https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html>.

Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-61 (1992) (citations omitted). Facebook challenges only the injury in fact requirement, which may be satisfied by allegations of either “actual or imminent” injury. *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 409 (2013). For an injury to be “imminent,” it must be “certainly impending” or there must be “a ‘substantial risk’ that the harm will occur.” *Id.* at 409 & n.5; *see also Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016), as revised (May 24, 2016) (noting that harm need not be tangible to be concrete).

1. Plaintiffs Have Suffered or Face a Substantial Threat of Identity Theft or Fraud.

Facebook’s assertion that Plaintiffs have articulated no theory of actual or cognizable harm, MTD 14, rings hollow in the face of Plaintiffs’ substantial allegations to the contrary and Facebook’s own notice to its users that their content and information had been improperly shared with Cambridge Analytica and others. That notice referenced keeping Plaintiffs’ data “safe,” acknowledged that “the website may have misused some of your Facebook information,” and said Facebook was “committed to confronting abuse,” tacitly admitting harm. Weaver Declaration, Ex. 2.

Here, all Plaintiffs allege concrete and particularized injuries that are actual or imminent. The scope of the information Facebook brokered, for its own gain, is far beyond that addressed in typical “data breach” cases that involve hacking of a few pieces of information. Facebook collects more than 52,000 unique data points about users and Facebook disclosed this extensive personal information to third parties, including dates and places of birth, photos with geolocating information, familial relationships, residence addresses, education, relationship and employment history. ¶¶ 112-13, 118-19, 123-29, 170-72, 366.⁷ Such information is commonly used for identity theft and fraud, especially where, as here, this data has been aggregated with other data sources. ¶¶ 399-401, 411. Through the Cambridge Analytica portal alone, Russian and other foreign and domestic operatives now possess users’ content and information, including private

⁷ Julia Angwin, et al., *Facebook Doesn’t Tell Users Everything It Really Knows About Them*, ProPublica (Dec. 27, 2016), <https://www.propublica.org/article/facebook-doesnt-tell-users-everything-it-really-knows-about-them>.

messages, photos and posts intended to be shared only with those to whom they were sent on the Facebook platform. ¶¶ 139, 146-50.

As a result, many Plaintiffs have already been victim of various forms of identity theft and fraud. Plaintiffs Paige Grays, Jason Ariciu, James Tronka, and Barbara Vance-Guerbe report phishing attempts, attempts to gain unauthorized access to their Facebook accounts, and Facebook friend requests from imposter accounts. ¶ 23-24, 55-58, 408. These events support Plaintiffs’ assertion that they are at substantial risk of imminent harm. Authority on which Facebook relies, MTD 17-18, found standing where the plaintiffs had alleged that they were placed at a “higher risk of ‘phishing’ and ‘pharming’ [which] are ways for hackers to exploit information they already have to get even more PII.” *In re Zappos.com, Inc.*, 888 F.3d 1020, 1027 (9th Cir. 2018).

Furthermore, Plaintiffs have paid for credit monitoring and incurred time and out-of-pocket costs to protect themselves from the substantial risk of identity theft and fraud. ¶ 412. Plaintiffs’ harm is compounded by Facebook’s failure to warn them of the unauthorized access and misuse of their personal information, which deprived Plaintiffs of an earlier opportunity to protect themselves against identity theft, fraud and manipulation. ¶¶ 312, 335-36, 374, 388, 412, 425, 431. These concrete harms are more than sufficient to confer standing.

Facebook sweepingly argues that “no court has ever accepted” the theory of “identity theft” standing pleaded here, MTD 1, but no defendant has ever so egregiously engaged in the harvesting of user content and information on such a broad scale and then sold access to it without authorization or consent. Moreover, the authorities on which Facebook relies do not limit Article III standing to disclosure of any particular type of personal information. All that is needed is “a credible threat of real and immediate harm” from the challenged conduct. *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010); *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) (standing exists where “the threatened injury is ‘certainly impending,’ or there is a ‘substantial risk’ that the harm will occur”); *see also Attias v. Carefirst, Inc.*, 865 F.3d 620, 628 (D.C. Cir. 2017) (plaintiffs established standing where they alleged a substantial

risk of identity fraud based solely on theft of health insurance subscriber ID numbers “even if their social security numbers were never exposed to the data thief”).⁸

2. Plaintiffs Have Suffered a Cognizable Injury to Their Privacy Interests.

In addition to substantially increasing Plaintiffs’ risk of identity theft, Facebook’s unauthorized disclosure of Plaintiffs’ personal information permanently damaged Plaintiffs’ privacy. ¶¶ 415-19. Facebook did not tell users that they would be subject to psychographic marketing, including the targeting of vulnerable communities for the purpose of manipulation, without revealing to users who was sending such targeted messaging. ¶¶ 368-98, 415. While Plaintiffs have spent and will have to spend resources to protect themselves from current and future identity theft and fraud, their content and information has already been released to third parties and cannot be retrieved. For that reason, it will be difficult if not impossible to extricate themselves from unwanted, outrageous targeted political and sales marketing.

These egregious, offensive privacy violations are sufficient to establish standing. *Van Patten v. Vertical Fitness Grp., LLC*, 847 F.3d 1037, 1043 (9th Cir. 2017) (noting that “[a]ctions to remedy defendants’ invasions of privacy, intrusion upon seclusion, and nuisance have long been heard by American courts,” and finding that the plaintiffs had Article III standing to pursue their privacy claim); *In re Google Inc. Cookie Placement Consumer Privacy Litig.* (“Google

⁸ Facebook’s other standing authorities concerning the wrongful disclosure of *non*-personally identifiable information are inapposite. See *In re SuperValu, Inc.*, 870 F.3d 763, 770 (8th Cir. 2017) (“the allegedly stolen Card Information does not include any personally identifying information”); *Goodman v. HTC Am., Inc.*, 2012 WL 2412070, at *7 (W.D. Wash. June 26, 2012) (rejecting standing based on misappropriation of location data); *Low v. LinkedIn Corp.*, 2011 WL 5509848, at *4 (N.D. Cal. Nov. 11, 2011) (rejecting standing based on browser history not “linked to his identity by LinkedIn” “anonymous LinkedIn user ID”); *LaCourt v. Specific Media, Inc.*, 2011 WL 1661532, at *4 (C.D. Cal. Apr. 28, 2011) (no standing for internet browsing “cookies” where no specific allegations supporting plaintiffs’ cookie “re-spawning” arguments). Plaintiffs here allege several categories of personally identifiable information. ¶¶ 119, 124, 154-55 (biographical information in addition to “name, gender, birthdate, location” exposed to third parties). Both the extent of the biographical information and the real and imminent risk of phishing and malicious fraudulent attack distinguish Plaintiffs’ allegations from *Antman v. Uber Technologies, Inc.*, 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015), where only drivers’ license information was disclosed.

Cookie Placement”), 806 F.3d 125, 134 (3d Cir. 2015) (noting that “the Supreme Court itself has permitted a plaintiff to bring suit for violations of federal privacy law absent any indication of pecuniary harm,” and finding that the plaintiffs had Article III standing to pursue privacy tort claims arising from the defendant’s web tracking activity).⁹

3. Plaintiffs Have Suffered Injury to Their Property Interests.

Courts recognize that economic injury includes “loss of value of PII,” which is the risk that personal data will become devalued once it is publicly disseminated. Facebook users’ personal information has significant economic value that is anything but “fanciful.” ¶ 409; MTD 8. Indeed, it should not come as any surprise to Facebook that Plaintiffs’ content and information has value, as that very content and information has generated billions of dollars in revenue for Facebook by way of advertising and other lucrative partnerships through which Facebook sells access to users’ data. Facebook calculates ARPU, meaning the average revenue each user generates for Facebook, derived from an analysis of the content and information each user shares.¹⁰ ¶¶ 400, 421. Thus, when users signed up to join Facebook, they were entering into a transaction—a value-for-value exchange in which users agreed to provide content that Facebook could use, subject to users’ privacy restrictions.

By allowing third parties access to users’ personal information—and effectively “making it ubiquitously available”—Facebook has diminished its value. ¶ 409. Because exclusive access to the information confers a competitive advantage, there is a “first user value” to this kind of

⁹ Facebook’s reliance on authorities finding lack of standing where the privacy violations are based only on the disclosure of and bare request for zip codes is misplaced. MTD 22 (citing *Spokeo*, 136 S. Ct. at 1550 (noting in the context of the Fair Credit Reporting Act, “[i]t is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm”); *Hancock v. Urban Outfitters, Inc.*, 830 F.3d 511, 514 (D.C. Cir. 2016) (“If, as the Supreme Court advised, disclosure of an incorrect zip code is not a concrete Article III injury, then even less so is Hancock and White’s naked assertion that a zip code was requested and recorded without any concrete consequence.”)).

¹⁰ Notably, the recently enacted California Consumer Privacy Act also recognizes the monetary value of personal information, providing that “[a] business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information.” Cal. Civ. Code § 1798.125(b)(1).

content and information. That value has now been lost. *See In re Anthem, Inc. Data Breach Litig.* (“*Anthem II*”), 2016 WL 3029783, *15 (N.D. Cal. May 27, 2016) (allegations of potential acts of fraud using plaintiffs’ PII “could be read to infer that an economic market existed...and that the value of [p]laintiffs’ PII decreased as a result of the [] data breach.”). Facebook is wrong, therefore, to argue that the individual Plaintiffs have failed to allege diminution in value of their content and information in order to establish damages. MTD 14-16, 20-21.¹¹

Facebook argues that, in order to establish injury-in-fact, Plaintiffs must plead they attempted to sell their personal information, that they would do so in the future or that they were injured by the loss of their ability to sell their own information at its market value. MTD 20-21.¹² Judge Koh declined to adopt this interpretation in *Anthem II*, finding, rather, that “Plaintiffs are

¹¹ Defendants’ cases are inapposite because all concern factual allegations that had legal defects. *See Birdsong v. Apple, Inc.*, 590 F.3d 955, 960 (9th Cir. 2009) (“The plaintiffs do not even claim that they used their iPods in a way that exposed them to the alleged risk of hearing loss.”); *Lewis v. Casey*, 518 U.S. 343, 358 (1996) (two isolated incidents of prisoners being denied ability to represent themselves does not support Arizona systemwide injunction following a trial); *Lierboe v. State Farm Mut. Auto. Ins. Co.*, 350 F.3d 1018, 1022 (9th Cir. 2003) (no standing when class representative had no claim against insurance company as a matter of law because “if Lierboe has no stacking claim, she cannot represent others who may have such a claim”); *In re iPhone Application Litig.*, 2011 WL 4403963, at *4 (N.D. Cal. Sept. 20, 2011) (“Plaintiffs do not identify what iDevices they used, do not identify which Defendant (if any) accessed or tracked their personal information, do not identify which apps they downloaded that access/track their personal information”); *Lujan*, 504 U.S. at 562 (plaintiff failed to establish standing at summary judgment because “when the plaintiff is not himself the object of the government action or inaction he challenges, standing is not precluded, but it is ordinarily ‘substantially more difficult’ to establish”); *Warth v. Seldin*, 422 U.S. 490, 504 (1975) (no standing to challenge prejudicial zoning ordinance because no plaintiff had pled a property interest). Here, Plaintiffs allege that they received notice that their content and information had been exposed through the Cambridge Analytica scandal.

¹² Facebook relies on authorities that concern far less intrusive conduct. *See In re Google, Inc. Privacy Policy Litig.*, 2013 WL 6248499, at *5 (N.D. Cal. Dec. 3, 2013) (no allegations that personal information was deliberately disclosed to business partners, only that Google combined personally identifiable information from various Google accounts); *In re Google Android Consumer Privacy Litig.* (“*Google Android Litig. I*”), 2013 WL 1283236, at *4 (N.D. Cal. Mar. 26, 2013) (“Plaintiffs do not identify which Android mobile devices they used and which of the Apps accessed and tracked their information.”); *Silha v. ACT, Inc.*, 807 F.3d 169, 174 (7th Cir. 2015) (plaintiffs voluntarily released personal information to schools and were only unaware test administrator would be paid).

not required to plead that there was a market for their PII *and* that they somehow also intended to sell their own PII,” but “to allege that there was either an economic market or that it would be harder to sell their own PII, not both.” 2016 WL 3029783, at *15; *See also Corona v. Sony Pictures Entm’t, Inc.*, 2015 WL 3916744, at *3 (N.D. Cal. June 15, 2015) (plaintiffs sufficiently pleaded economic injury where “the[ir] PII was stolen and posted on file-sharing websites for identity thieves to download”).¹³

B. Plaintiffs Did Not Consent to Facebook’s Disclosure of Personal Information.

Facebook defends its unauthorized disclosure of personal information by maintaining that Plaintiffs consented to its misconduct. Proving consent is Facebook’s burden, which it has failed to meet. *See, e.g., Matera v. Google Inc.*, 2016 WL 5339806, at *17 (N.D. Cal. Sept. 23, 2016).

1. Users Did Not Consent to the Privacy and Data Use Policies When They Opened a Facebook Account.

On the Internet as elsewhere, mutual assent is the touchstone of contract. *Long v. Provide Commerce, Inc.*, 245 Cal. App. 4th 855, 862 (2016). Here it was missing. California applies an objective standard to determine mutual assent, looking to the “reasonable meaning” of the parties’ “words and acts.” *Id.* The reasonable meaning of opening a Facebook account during the Class Period did not include agreement to the Privacy and Data Use Policies.¹⁴

From March 2009 until February 2012, Facebook’s sign-up process involved two screens. The first required users to enter their name, email, password, gender, and birthday.

¶ 261. Users could not continue beyond the first screen until they filled in each field and clicked the “Sign Up” button. *Id.* No reference to any Policy appeared on this page. *See id.* Upon clicking “Sign Up,” users were routed to a “Security Check” page where users were required to

¹³ Facebook’s other authorities supporting its argument that Plaintiffs’ lack standing for failure to plead harm and damages do not actually address standing questions. *Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 912 (N.D. Cal. 2009) (plaintiffs in identity theft case had standing based on risk of future harm); *see also Frangipani v. Boecker*, 64 Cal. App. 4th 860 (1998) (not addressing standing issues); *Aguilera v. Pirelli Armstrong Tire Corp.*, 223 F.3d 1010, 1015 (9th Cir. 2000) (same).

¹⁴ The “Privacy Policy” was relabeled to the “Data Policy,” and then relabeled again as the “Data Use Policy.” ¶ 242, note 69.

enter the text from a text CAPTCHA.¹⁵ Underneath the text CAPTCHA was a “Sign Up” button, and, in small font beneath that button was text stating that by clicking “Sign Up,” users were indicating that they had “read and agreed to the Terms of Use [hyperlinked] and Privacy Policy [hyperlinked].” ¶ 264.

This was not a classic clickwrap agreement, as Facebook used prior to March 2009, where, to proceed, users had to click a box separately affirming that they had read and agreed to the Terms of Use and Privacy Policy. ¶¶ 258-61. Rather, it was a “sign-in-wrap” agreement, which purports to bind users to terms when they click the sign-up button. *See Berkson v. Gogo LLC*, 97 F. Supp. 3d 359, 399 (E.D.N.Y. 2015). While the Ninth Circuit and California courts have not directly addressed sign-in-wrap agreements, the Second Circuit, applying general principles of contract law, has held that a sign-in-wrap “binds users only when ‘the design and content’ of the webpage ‘render[s] the existence of terms reasonably conspicuous.’” *Nicosia v. Amazon.com, Inc.*, 834 F.3d 220, 233 (9th Cir. 2016) (quoting *Nguyen v. Barnes & Noble, Inc.*, 763 F.3d 1171, 1177-78 (9th Cir. 2014)).

Here, the design of the webpage gave users no reason to notice the small print referring to the Terms of Use and Privacy Policy. Facebook featured the text CAPTCHA and the second Sign Up button, while the policy reference was in a miniscule font without bolding or highlighting to draw the eye. *See* ¶¶ 263-64. The existence of references to the Terms of Use and Privacy Policy were not reasonably conspicuous—at the very least, reasonable minds could disagree on whether they were. *See* ¶ 237. In any event, by the time users reached the reference, they had already entered personal information, clicked “Sign Up” once, and deciphered a text CAPTCHA, giving little reason to notice text and hyperlinks beneath a second “Sign Up” button. ¶¶ 261-64.

For the rest of the Class Period—from February 2012 until April 2018—a single sign-up page collected personal information and referred users to the Terms of Use and Data Use Policy

¹⁵ A text CAPTCHA is a program that uses distorted text to verify that a human, not a computer, is entering data. Deb Amlen, *What the Heck Is That?: CAPTCHA*, N.Y. Times (Feb. 26, 2018), <https://www.nytimes.com/2018/02/26/crosswords/what-the-heck-is-that-captcha.html>.

through text located above the “Sign Up” button. Facebook also changed the reference text, which stated that “[b]y clicking Sign Up” or “Create Account,” users “agree to our Terms [hyperlinked]” and “that [they] have read” (—or, from February 2012 to May 2012, “read and understand”)—“our Data Use Policy [hyperlinked].” ¶¶ 266-68. The new reference text only asked users to agree that they had read, or read and understood, the Data Use Policy. The absence of any request for agreement to the Data Use Policy itself would lead reasonable readers to conclude that Facebook was not seeking their consent to the Data Use Policy. Thus, the “contractual nature” of the Data Use Policy was “not obvious.” *Windsor Mills, Inc. v. Collins & Aikman Corp.*, 25 Cal. App. 3d 987, 993 (1972).¹⁶

2. Users Did Not Consent to the Privacy and Data Use Policies Through the SRR.

Facebook argues that users agreed to the Privacy Policies and Data Use Policies because they were incorporated by reference in the SRR. But Facebook overlooks what is required to incorporate a separate document into a contract by reference: “the reference must be clear and unequivocal, the reference must be called to the attention of the other party and he must consent thereto, and the terms of the incorporated document must be known or easily available to the contracting parties.” *Wolschlag v. Fid. Nat’l Title Ins. Co.*, 111 Cal. App. 4th 784, 790 (2003) (internal quotation marks and citation omitted). In the context of incorporation by reference, as elsewhere, “mutual consent is an essential element of any contract.” *Avery v. Integrated Healthcare Holdings, Inc.*, 218 Cal. App. 4th 50, 67 (2013). And if an “offeree reasonably [does] not know that an offer ha[s] been made,” there cannot be consent to that offer. *Norcia v. Samsung Telecomms. Am.*, 845 F.3d 1279, 1285 (9th Cir. 2017).

¹⁶ A court in this district has expressed concern about the use of a single “Sign Up” click to activate an account and accept terms of service, reluctantly concluding that clicking “Sign Up” was enough to manifest assent. *See In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155, 1166 (N.D. Cal. 2016). The court based this conclusion not on a Ninth Circuit holding, but from a citation in a Ninth Circuit opinion. *See id.* (noting that *Nguyen*, 763 F.3d at 1176-77, had cited *Fteja v. Facebook, Inc.*, 841 F. Supp. 2d 829, 838-40 (S.D.N.Y. 2012)). District courts, however, are bound by what the Ninth Circuit has held, not what it has cited. And nothing the Ninth Circuit has held suggests that the inconspicuous reference to the Terms of Use and Privacy Policy bound users to the Privacy Policy.

The issue is not merely that the SRR failed to use the term “incorporate.” Reasonable readers did not know that the offer to contract included the Data Use or Privacy Policies, because there was no hint that those Data Use Policies were intended to bind the parties. The SRR said that the Data Use Policies were intended “to make important disclosures,” not to create obligations. Readers of the SRR were not directed or required to read the Policies, but “encourage[d]” to do so. ¶ 243. Mentioning the Data Use Policies “is not the same as specifically directing the parties’ attention to the terms of the external document in a manner that could be construed as eliciting the parties’ consent to its separate terms.” *Amtower v. Photon Dynamics, Inc.*, 158 Cal. App. 4th 1582, 1609 (2008). Nothing in the reference to the Data Use Policies “notif[ied] the consumer that” use of Facebook “would be considered agreement to the terms set forth in the” Data Use Policies. *Norcia*, 845 F.3d at 1287. For this reason, Plaintiffs did not consent to the terms of the Policies.

The SRR’s reference to the Data Use Policies is worlds apart from the two cases on which Facebook heavily relies: *Wolschlager* and *Shaw v. Regents of University of California*, 58 Cal. App. 4th 44 (1997). The contracts in both of those cases alerted readers that they were consenting to terms contained in other documents. In *Shaw*, the contract expressly mentioned that the signing party would retain his rights under the attached document, thus making it clear that the document was intended to be part of the contract. *See Shaw*, 58 Cal. App. 4th at 856; *see also Amtower*, 158 Cal. App. 4th at 1609 (discussing *Shaw*). In *Wolschlager*, the question was whether a preliminary title report incorporated an arbitration clause in a title insurance policy. There, it was both “the express direction to the insured to read the policy,” and the fact that “the insured had solicited the preliminary report for the very purpose of obtaining the policy” that “clearly indicated that the terms of the policy applied to any action based upon the preliminary report.” *Amtower*, 158 Cal. App. 4th at 1608. The insured in *Wolschlager* necessarily knew that his consent included consent to the title policy.

At a minimum, the SRR was unclear as to whether it was seeking consent to the Policies. Ambiguities in the SRR must be construed against the drafter: Facebook. For that reason alone,

the SRR did not incorporate the Policies. *See Chan v. Drexel Burnham Lambert, Inc.*, 178 Cal. App. 3d 632, 644 (1986) (construing purported incorporation against drafter).

3. The Privacy and Data Use Policies Did Not Disclose Third-Party Access to Their Content and Information Through Their Friends.

Even if users *had* agreed to the Data Use Policy, users—contrary to Facebook’s argument—would not have consented to Facebook’s misconduct, expressly or otherwise. The “question of express consent is usually a question of fact, where a fact-finder needs to interpret the express terms of any agreements to determine whether these agreements adequately notify individuals” regarding the conduct at issue. *In re Google Inc. Gmail Litig.*, 2014 WL 1102660, at *15 (N.D. Cal. Mar. 18, 2014). For this reason, at the pleading stage, courts have refused to accept Facebook’s argument that users “consented” to challenged conduct on the basis of its SRR or Data Policy. *See Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 806 (N.D. Cal. 2011). Moreover, with respect to invasion of privacy and similar claims, “consent is only effective if the person alleging harm consented ‘to the particular conduct, or to substantially the same conduct’ and if the alleged tortfeasor did not exceed the scope of that consent.” *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1072-73 (N.D. Cal. 2016) (quoting Restatement (Second) of Torts § 892A (1979) §§ 2(b), 4)); *see also Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 847-48 (N.D. Cal. 2014) (“[C]onsent with respect to the processing and sending of messages itself does not necessarily constitute consent to the specific practice [of] the scanning of message content for use in targeted advertising.”).

No document on Facebook’s website “clearly and prominently disclosed” that Facebook allowed its business partners to download users’ content and information if third parties engaged with them. Facebook shows no screenshot that reflects this. The hard copy policy documents Facebook asks the Court to consider contain numerous false, misleading statements that contradict what a reasonable user understood to be the contract. For example, the SRR represented that users “own all of the content and information [they] post on Facebook and [they] can control how it is shared.” ¶¶ 219-22. It told users that, “[w]hen you share and communicate using our Services, you choose the audience who can see what you share.” ¶ 276.

Facebook promised that “applications [would] respect your privacy,” and that applications accessing the data of a friend “will only be allowed to use that content and information in connection with that friend.” ¶¶ 225, 274. Facebook’s site falsely stated that it “do[es] not give your content or information to advertisers without your consent.” ¶¶ 228-30, 232-33. These all nurtured deception by omission.

To rationalize giving app developers access to user content and information, Facebook points to a disclosure in its Data Use Policy stating that Facebook “require[s] applications to respect your privacy,” and that applications accessing the data of a friend “will only be allowed to use that content and information in connection with that friend.” ¶¶ 225, 274. This, Facebook says, should have informed users that, when users’ friends downloaded an app, that app could access all of the content and information the user shared with that app. This argument fails. For one thing, Facebook’s convoluted phrasing does not express clearly that friends could share users’ data, and thus does not “constitute[] a clear consent by users.” *See Cohen v. Facebook, Inc.*, 798 F. Supp. 2d 1090, 1094-96 (N.D. Cal. 2011). Further, in the context of all of Facebook’s other representations about privacy, no reasonable user would have expected friends’ sharing to override other privacy controls and promises. *See infra* Section II.F.

Facebook also points to a sentence in one of three different policies that refers to permissions given to applications to share user content and information. That sentence appears only in Facebook’s Data Use Policy from September 7, 2011 to January 30, 2015 (and so could not apply to users who signed up before or after that time): “if you’ve shared your likes with just your friends, the application could ask your friend for permission to share them.” ¶ 275. But this opaque sentence was never included in the main terms of service, and exemplifies how Facebook introduced multiple versions of extremely lengthy collateral policies that changed terms, without notice to users, at Facebook’s whim. In any event, that phrase did not tell users that app developers would have full access to all of the content and information, including, for example, time-stamped and geolocated photos sent privately through Facebook messenger.

Nor does Facebook point to any specific disclaimer on its site that affirmatively informed users that if a friend engaged with Facebook’s business partners—such as Qualcomm, Amazon, and Huawei—these business partners were given access to a user’s content and information, including user ID, birthday, work, and education history. ¶¶ 112-14, 173. The statements in the Data Use Policy—even if binding on users—do not clearly communicate that one’s own privacy settings are overruled and, for example, content shared with a friend would be shared with Amazon, if that friend logs in to Amazon through Facebook. The Data Use Policy’s statement that Facebook may “give your information to the people and companies that help us provide, understand, and improve the services we offer” and “may use outside vendors to help host our website, serve photos and videos, process payments” is far from a clear disclosure to users that Facebook gave their data to every major mobile carrier in the world. ¶¶ 281-84. Nor is Facebook helped by the statement that its “partners” (who, *contra* Facebook, are not just device makers) must comply with the “agreements we enter into with them.” Those agreements are not shared with users, so users do not know their provisions.

All these issues raise questions of fact regarding meaningful consent. Facebook has not met its burden of showing as a matter of law that Plaintiffs expressly consented to the particular sharing at issue here—the sharing of their content and information with third-party apps and business partners. *See Matera*, 2016 WL 5339806, at *18 (“Google has not shown that Gmail users consent to the interception, scanning, and analysis of email for purposes of creating targeted advertising for non-Gmail users.”); *Campbell*, 77 F. Supp. 3d at 847-48 (noting that consent with respect to one use is not necessarily consent with respect to another); *Cohen*, 798 F. Supp. 2d at 1094-96 (“Facebook has not established that [the plaintiffs] consented to the particular uses in dispute here.”).

4. The Language Facebook Claims Disclosed and Obtained Consent Was Contradicted in the User Experience by the Privacy Settings.

Even if users understood that *publicly* posted content would be shared, it is not reasonable to construe these disclosures as applying to status updates, likes, photographs, and other communications that Plaintiffs configured to be non-public by selecting a non-public

audience at the time of posting or by choosing to make a category of content non-public through Facebook's Privacy Settings. *See Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659, 668-69 (D.N.J. 2013) (“[W]hen users make their Facebook wall posts inaccessible to the general public, the wall posts are ‘configured to be private.’”). When users make a category of data non-public they have not consented to Facebook disclosing that data to third parties. This was precisely the Supreme Court of California's conclusion with respect to the Stored Communications Act (“SCA”) in *Facebook, Inc. v. Superior Court*, 4 Cal. 5th 1245, 1276-81 (2018); *see also Ehling*, 961 F. Supp. 2d at 668-69 (“[N]on-public Facebook wall posts are covered by the SCA.”). Facebook's contrary “view would effectively eliminate expectations of privacy in all communications and hence would undermine the privacy rights of all users.” *Facebook, Inc. v. Superior Court*, 4 Cal. 5th at 1278.

Fundamentally, where, as here, users are promised privacy, consent to Facebook allowing third-party content and information access is lacking. *See In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1070-71 (N.D. Cal. 2012) (at the pleading stage, accepting plaintiffs' argument “that, in light of Apple's statements about protecting user privacy, Plaintiffs did not expect or consent to the tracking and collecting of their app use or otherwise personal information”). Facebook's “privacy controls” were designed to give the appearance that users could limit who had access to their content and information. ¶¶ 184-91.

Facebook told users they could make their content and information “public,” allowing everyone to view it; or they could restrict access to specific Facebook friends. *Id.* This was not true. Facebook set default settings such that users who wanted to prevent Facebook from sharing their information with app developers had to affirmatively disable access to the 15 categories of personal information that were by default shared with applications used by friends. This process required users to (1) click on the link to Facebook's Settings webpage; (2) click on the link to the App Settings webpage; (3) click on the link to edit settings for “Apps others use”; (4) deselect each of the 15 categories of information enabled by default; and (5) click “Save Changes.” ¶¶ 193-98. Even then, Facebook would still share a user's name, gender, and friend list with

applications used by friends, unless that user disabled application access altogether—an option that was confusingly located in a different subpage of Facebook’s App Settings. ¶¶ 199-201. Moreover, these settings had no effect whatsoever on the access Facebook provided to third-party business partners like Amazon. ¶ 169. And, when an application obtained access to a user’s content and information through a user’s friend, the user was not notified, or given the opportunity to block or opt out of such access. ¶¶ 183, 196, 299. Knowing consent would have informed users each time their data was being accessed by a third party as well as the identity of that third party, so a user could accept or refuse that access. Facebook does not argue otherwise.

C. Facebook Cannot Hide Behind an Exculpatory Clause.

Facebook maintains that an exculpatory clause in the SRR bars all claims based on third-party conduct, relying on a provision that “Facebook is not responsible for the actions . . . of third parties.” MTD 13. The conduct at the heart of Plaintiffs’ complaint, however, is Facebook’s, not that of third parties. Facebook gave third parties the data; they did not steal it. *In re Facebook PPC Advert. Litig.*, 2010 WL 3341062, at *5 (N.D. Cal. Aug. 25, 2010) (holding “disclaimer does not cover [Facebook’s] own actions”); *Bailey v. United States*, 289 F. Supp. 2d 1197, 1212 (D. Haw. 2003) (distinguishing “situation in which a party seeks a waiver of liability for its own actions”).

Moreover, an exculpatory clause cannot bar claims for violations of statutory law or claims sounding in gross negligence or fraud. *See City of Santa Barbara v. Superior Court*, 41 Cal. 4th 747, 776-77 (2007).

Even if the claims involved third parties’ conduct, the SRR’s exculpatory clause is invalid under *Tunkl v. Regents of University of California*, which set out six public interest factors that invalidate exculpatory clauses. 60 Cal. 2d 92, 97-102 (1963) (noting contract at issue “need only fulfill some” of six characteristics to invalidate exculpatory clause).

Facebook’s SRR meets all of those factors. Facebook performs a “service of great importance to the public” that for some is a “practical necessity.” *Id.* at 98-99. According to Mark Zuckerberg, Facebook is not just “a powerful new tool [for people] to stay connected to the

people they love,” but is also an essential forum for public discourse and commerce—a way for users “to make their voices heard,” “build communities,” raise funds for charity, organize social movements, and run 70 million small businesses.¹⁷ See ¶¶ 1, 560(B). A service need not be a “necessity of life” for it to be a “practical necessity” under *Tunkl*. See *Pelletier v. Alameda Yacht Harbor*, 188 Cal. App. 3d 1551 (1986) (invalidating exculpatory clause related to yacht berth). Facebook likewise “possesses a decisive advantage of bargaining strength” against users due to the essential nature of the service. 60 Cal. 2d at 100. Users cannot go elsewhere for comparable services. The sheer number of Facebook users—2.2 billion—creates a network effect that no other social media platform has been able to replicate.

Facebook holds itself out as willing to provide services “for any member of the public who seeks it,” *Tunkl*, at 98-99, and its SRR is “a standardized adhesion contract,” *id.* at 100. Facebook users’ data is also placed “under the control” of Facebook and is “subject to the risk of carelessness” by Facebook. *Id.* at 101. As explained in Section II.B.4, Facebook users have no meaningful control over their data. See ¶¶ 184-210. Finally, Facebook’s business is “of a type generally thought suitable for public regulation.” *Tunkl*, 60 Cal. 2d at 98. It is subject to Federal Trade Commission (“FTC”) regulation, ¶¶ 294-300, and an intricate web of laws.¹⁸ See *Gardner v. Downtown Porsche Audi*, 180 Cal. App. 3d 713, 717 (1986) (auto repair shop is business suitable for public regulation).

Finally, Facebook’s contractual waiver is procedurally and substantively unconscionable. Procedurally, the provision is oppressive due to users’ complete lack of bargaining power, and substantively, it is one-sided. See, e.g., *A & M Produce Co. v. FMC Corp.*, 135 Cal. App. 3d 473, 493 (1982) (affirming holding of unconscionable disclaimer provision where “nonnegotiable terms on preprinted form agreements combine with disparate bargaining power [and] result[] in

¹⁷ Testimony of Mark Zuckerberg Before the H. Comm. on Energy & Commerce, 2018 WL 1740473 (Apr. 11, 2018).

¹⁸ For example, Facebook is subject to the Children’s Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506, the Illinois Biometric Information Privacy Act of 2008, 740 Ill. Comp. Stat. 14/1, and the recently enacted California Consumer Privacy Act of 2018, 2018 Cal. Legis. Serv., ch. 55.

the allocation of commercial risks in a socially or economically unreasonable manner”); *Lhotka v. Geographic Expeditions, Inc.*, 181 Cal. App. 4th 816, 826 (2010) (limitation of liability provision was unconscionable).

D. Facebook Violated Federal Statutes.

1. Plaintiffs Have Standing to Bring VPPA and SCA Claims.

Plaintiffs have standing to bring claims under the Video Privacy Protection Act (“VPPA”), 18 U.S.C. § 2710 (2012), and the Stored Communications Act (“SCA”), *id.* §§ 2701-11. Where a statute codifies a substantive right—and certainly where it codifies a privacy right whose violation has long been recognized as a freestanding injury, as do the VPPA and SCA—plaintiff need not plead any additional harm beyond a violation of the statute to obtain standing. *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017). The Ninth Circuit evaluates whether the statute establishes a “substantive right,” and, if so, whether every violation of the statute “presents the precise harm and infringes the same [substantive] interests” the legislature sought to protect by enacting the statute. *Id.* at 983-84; *see Spokeo*, 136 S. Ct. 1540; *see also In re iPhone Application Litig.*, 844 F. Supp. 2d at 1055. The Ninth Circuit and this Court have held that violations of the VPPA and the SCA are thus sufficient to establish an injury under Article III in the Ninth Circuit. *Eichenberger*, 876 F.3d at 983; *see also Spokeo*, 136 S. Ct. 1540; *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1055. Facebook’s wrongful and unlawful conduct has injured Plaintiffs and caused them to incur damages that establish Article III standing under *Spokeo*.

2. Facebook Violated the VPPA.

a. Facebook is a Video Tape Service Provider Under the VPPA.

Facebook is a “video tape service provider” under the VPPA. 18 U.S.C. § 2710(a)(41); *Eichenberger*, 876 F.3d at 983. Facebook is wrong that courts have interpreted this term narrowly. As a court in this district has ruled, Congress intended “to cover new technologies for pre-recorded video content,” so that the VPAA’s protections would retain their force even as technologies evolve.” *In re Hulu Privacy Litig.*, 2012 WL 3282960, at *6 (N.D. Cal. Aug. 10,

2012). In holding that Hulu was a video tape service provider, the court concluded, “a plain reading of a statute that covers videotapes and ‘similar audio visual materials’ is about the video content, not about how that content was delivered (e.g., via the Internet or a bricks-and-mortar store).” *Id.* at *5. Other courts in this Circuit have also interpreted the term broadly. *See In re Vizio, Inc., Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1213 (C.D. Cal. 2017) (holding that Smart TV companies are video tape service providers); *Amazon.com v. Lay*, 758 F. Supp. 2d 1154, 1170 (W.D. Wash. 2010) (finding Amazon qualifies as video tape service provider under VPPA). A passing comment in *Lane v. Facebook*, made while evaluating a class-action settlement, is irrelevant here. 696 F.3d 811, 823 (9th Cir. 2012).

b. Facebook User Data Is Personally Identifiable Information Under the VPPA.

The user information Facebook disclosed to third parties was “personally identifiable information” under the VPPA, which defines the term to “include[] information which identifies a person as having *requested* or *obtained* specific video materials or services from a video tape service provider.” 18 U.S.C. § 2710(a)(3). Facebook disclosed to third parties, videos its users both “liked” and watched. ¶¶ 119, 124-26 (describing numerous categories in Graph API v.1.0 that included a user’s likes and video viewing history). A Facebook user’s “like” of a video indicates that the user “requested or obtained” the video he or she liked. 18 U.S.C. § 2710(a)(3). And since Facebook also disclosed the user’s name and profile photo, which could have been used to identify that user, Facebook disclosed “information which identifie[d]” the user. *Id.*; *see also Eichenberger*, 876 F.3d at 984. The cases Facebook cites do not defeat Plaintiffs’ claim. *Gonzalez v. Cent. Elec. Coop.*, 2009 WL 3415235, at *11 (D. Or. Oct. 15, 2009) (finding evidence indicating “plaintiff purchased one of fifteen movies does not constitute personally identifiable information”); *In re Hulu Privacy Litig.*, 2014 WL 1724344, at *1 (N.D. Cal. Apr. 28, 2014) (holding no VPPA violation where “user’s identity and that of the video material were transmitted separately”).

While Facebook did disclose information sufficient to indicate which videos its users watched, Facebook is wrong that the VPPA provides privacy only to Americans’ actual viewing

history. Indeed, the information about Robert Bork that prompted enactment of the VPPA disclosed only Judge Bork's rental history, not confirmation of actual viewing.

c. Plaintiffs Did Not Consent to the Disclosure of Their Data Under the VPPA.

Facebook wrongly asserts that users consented to disclosure of their data under 18 U.S.C. § 2710(b)(2), which authorizes disclosures to third parties only with the consumer's "informed, written consent" that is "distinct and separate" from any form setting out the consumer's "legal and financial obligations," and is either "given at the time disclosure is sought" or given in advance for a set period of time that cannot exceed two years. 18 U.S.C. § 2710(b)(2)(B). Even if the purported generalized user "consent" Facebook seeks to invoke were adequate to foreclose other of Plaintiffs' claims—which, as discussed above, it is not—that consent would be wholly inadequate under the VPPA. Facebook does not obtain informed, written consent distinct from the SRR or policies, either at the time Facebook sought to disclose the user's video viewing history or in advance and for a set duration. *See In re Hulu Privacy Litig.*, 2014 WL 2758598, at *18 (N.D. Cal. June 17, 2014) (holding that Facebook data policy did not qualify as VPPA consent); *In re Hulu Privacy Litig.*, 2014 WL 1724344, at *17 (same).

3. Facebook Violated the Stored Communications Act.

Plaintiffs properly plead that Facebook violated the SCA by (i) knowingly divulging the contents of Plaintiffs' electronic communications while they were in electronic storage to unauthorized parties; and (ii) knowingly divulging the contents of Plaintiffs' electronic communications that were carried or maintained on Facebook's remote computing service to unauthorized parties. ¶¶ 449-73.¹⁹ Facebook does not contest that the SCA applies or that it knowingly divulged Plaintiffs' communications. Its remaining arguments fail.

To begin with, Plaintiffs did not consent to Facebook's distribution of their personal information to app developers and other third parties through friends. Facebook argues only that Plaintiffs provided express consent—not implied consent—to its sharing of information, but as

¹⁹ Plaintiffs allege that Facebook violated SCA sections 2702(a)(1) and 2702(a)(2) and agree that Facebook's conduct does not constitute a violation of section 2701(a). *See* MTD 29-30.

discussed in Section II.B above, it has not established consent. *See, e.g., Matera*, 2016 WL 5339806, at *17 (under the Wiretap Act, “as the party seeking the benefit of the exception,” defendant bears the burden of showing consent). Plaintiffs have sufficiently alleged that they were not aware of and did not consent to the sharing of their information with third parties, including app developers. ¶¶ 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 65, 67, 69, 71, 73, 75, 77, 79, 81, 83, 85, 87.

Even if the Court accepted Facebook’s argument regarding express consent, any such consent would be inapplicable to communications—including status updates, likes, photographs, and videos—that Plaintiffs configured to be non-public, either by selecting a non-public audience at the time of posting or by choosing to make a category of information non-public through Facebook’s Privacy Settings. *Facebook, Inc. v. Superior Court*, 4 Cal. 5th at 1276-81; *Ehling*, 961 F. Supp. 2d at 668-69 (“[N]on-public Facebook wall posts are covered by the SCA.”).

Facebook also argues that Plaintiffs’ SCA claim should be dismissed because “Plaintiffs have not alleged that any of their Facebook information was set to anything other than ‘public.’” MTD 30. The Court cannot accept Facebook’s apparent argument—that each of the 34 named Plaintiffs configured all of their posts and information to be public—while making all reasonable inferences in Plaintiffs’ favor. That argument is also belied by the fact that Facebook has access to all of Plaintiffs’ posts and information, yet has not affirmatively asserted that all of these posts and information have been configured to be public. In addition, all Plaintiffs allege that they used Facebook’s instant messaging service, which is by definition a private, non-public communication platform. *See* ¶¶ 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 65, 67, 69, 71, 73, 75, 77, 79, 81, 83, 85, 87. Facebook responds that app users “authorized the app,” MTD 30, but fails even to argue, much less to show as a matter of law, that app users consented to the disclosure of their *messages* to app developers.

Contrary to Facebook’s assertion, Plaintiffs clearly allege that their “content and information” may have been or was likely “‘shared’ with and ‘misused’ by the This is Your

Digital Life app.” See ¶¶ 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 65, 67, 69, 71, 73, 75, 77, 79, 81, 83, 85, 87; cf. MTD 30. First, Facebook admits that the Complaint alleges that This Is Your Digital Life obtained information on Plaintiffs’ “likes.” MTD 30-31. More importantly, Facebook ignores the fact that Plaintiffs challenge its unlawful disclosure of personal information—including education history, interests, likes, notes, relationship details, religion and politics, status updates, videos, and work history—to *all* applications that obtained unauthorized access to such information, including the This Is Your Digital Life app, as well as Facebook’s business partners. ¶¶ 124, 218, 338, 522. Facebook offers no argument regarding its disclosure of these additional categories of information.

E. Plaintiffs’ Privacy Claims Should Be Upheld.

1. Facebook’s General Challenges to Plaintiffs’ Privacy Claims Are Unavailing.

First, Facebook challenges Plaintiffs’ claims for invasion of privacy by intrusion into private affairs and for violation of Article I, Section I of the California Constitution, arguing that Plaintiffs have not alleged a *reasonable expectation of privacy* “because they consented to the disclosure of the information.” MTD 37. However, as set forth in Section II.B above, each of Facebook’s arguments regarding consent are unavailing and should be rejected.

Second, Facebook argues that Plaintiffs’ claims for invasion of privacy by public disclosure of private facts and for invasion of Article I, Section I of the California Constitution should be dismissed because “Plaintiffs have not demonstrated a legally protected privacy interest,” in that they have not specified what sensitive information was disclosed. MTD 37-39. However, Plaintiffs allege that Facebook disclosed numerous categories of sensitive content and information to app developers and other third parties, including name, Facebook User ID, education history, interests, likes, notes, photos, relationship details, religion and politics, status updates, videos, and work history. ¶¶ 3, 3 n.2, 21-88, 119, 123-24, 580-87. The material that Facebook disclosed, including personal family photographs, is clearly “sensitive.” See *Hughey v. Drummond*, 2015 WL 4395013, at *11-12 (E.D. Cal. July 16, 2015) (finding a legally protected privacy interest in materials containing “personal family photos and other personal electronic

files”); *Facebook, Inc. v. Superior Court*, 15 Cal. App. 5th 729, 738 (2017) (analogizing Facebook posts to private holiday greeting cards, which may inform friends and relatives “of highly personal events such as births, deaths, illness or job loss,” and may include “personal photographs”).²⁰

Third, Plaintiffs have clearly alleged conduct that would be “highly offensive to a reasonable person,” for purposes of their common-law privacy claims.²¹

In determining the “offensiveness” of an invasion of a privacy interest, common law courts consider, among other things: the degree of the intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder’s motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded.

Hill v. NCAA, 7 Cal. 4th 1, 26 (1994); *see also Opperman v. Path*, 205 F. Supp. 3d 1064, 1077 (N.D. Cal. 2016) (upholding plaintiffs claim for invasion of privacy where defendant uploaded plaintiffs’ email address book without consent); *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272 (2009); *Miller v. Nat’l Broad. Co.*, 187 Cal. App. 3d 1463, 1483-84 (1986). Here, every factor weighs in favor of finding that Facebook’s conduct was highly offensive: Facebook intruded upon a vast array of information regarding Plaintiffs, including personal and family photographs; it did so despite Plaintiffs’ express designation of such information as non-public, rather than public; Facebook misrepresented its practices and policies regarding data sharing to Plaintiffs; it

²⁰ The cases cited by Facebook are readily distinguishable. *See* MTD 37 (citing *Zbitnoff v. Nationstar Mortg., LLC*, 2014 WL 1101161, at *4 (N.D. Cal. Mar. 18, 2014) (concerning credit check for mortgage voluntarily obtained); *Scott-Codiga v. Cty. of Monterey*, 2011 WL 4434812, at *7 (N.D. Cal. Sept. 23, 2011) (concerning unspecified facts about a person’s employment recognizing “confidential and sensitive” privacy interest in emails but alleging no such use); *In re Yahoo! Mail Litig.*, 7 F. Supp. 3d 1016, 1041 (N.D. Cal. 2014) (plaintiffs relied upon a conclusory allegation that their emails were “private” without stating facts related to what particular emails were intercepted or the content within such emails)). Here, all Plaintiffs allege use of Facebook which entails a wealth of personal information not contained in email messages.

²¹ Facebook attempts to conflate the “highly offensive to a reasonable person” standard applicable to Plaintiffs’ common-law claims with the “egregious breach of social norms” standard applicable to Plaintiffs’ California Constitution claim, and offers no substantive argument regarding the former. MTD 37-39.

intruded into a space where Plaintiffs shared personal information, in which they had a reasonable expectation of privacy; and Facebook committed this intrusion for its own commercial benefit—to attract and obtain advertising revenue. The highly offensive nature of Facebook’s intrusion is also “evidenced by the intense public outcry and numerous, international governmental investigations in response to Defendants’ invasions of Plaintiffs’ and Class Members’ privacy rights,” as is detailed in the Complaint. *See* ¶ 517.

Fourth, Plaintiffs have alleged conduct that is “sufficiently serious” to constitute an “egregious breach of social norms” under Article I, Section I of the California Constitution. *Hill*, 7 Cal. 4th at 37; *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2011). Where, as here, a defendant has not only violated privacy interests, but also misled plaintiffs into believing that it will protect their privacy choices, claims for violation of the California Constitution have been upheld. *See, e.g., Google Cookie Placement*, 806 F.3d at 150-51. In *Google Cookie Placement*, the defendant had tracked users’ URLs even though plaintiffs had installed cookie blockers designed to prevent the tracking. In determining the egregiousness of the breach, the court reasoned that “Google not only contravened the cookie blockers—it held itself out as respecting the cookie blockers”; further, “users are entitled to deny consent, and they are entitled to rely on the public promises of the companies they deal with.” *Id.* at 151; *see also Goodman*, 2012 WL 2412070, at *14 (finding egregious breach where defendant used location tracking data to “build profiles about [plaintiffs] and sell this information to third parties”).²² Like *Google Cookie Placement*, here, Facebook’s affirmative promises of security and its dubious “privacy”

²² Facebook relies on cases dissimilar to the facts at hand, involving either data breaches or the sharing of application users’ information—not the information of such users’ friends. *See* MTD 37-38 (citing *Razuki v. Caliber Home Loans, Inc.*, 2018 WL 2761818, at *2 (S.D. Cal. June 8, 2018) (plaintiffs information obtained during data breach); *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1127-28 (N.D. Cal. 2008) (third party stole laptop containing plaintiffs’ personal information from defendant); *Gonzales v. Uber Techs., Inc.*, 2018 WL 1863148, at *10 (N.D. Cal. Apr. 18, 2018) (sharing of information by users of application); *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1063 (same); *Google Android Litig. I*, 2013 WL 1283236, at *11 (same); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (same); *Yunker v. Pandora Media, Inc.*, 2013 WL 1282980, at *15 (N.D. Cal. Mar. 26, 2013) (same)).

settings misled users into believing they could control who accessed their content and information. This type of misleading behavior constitutes an egregious breach of Plaintiffs' right to privacy.

2. Plaintiffs State a Claim for Public Disclosure of Private Facts.

Facebook invaded Plaintiffs' right to privacy by publishing Plaintiffs' private content and information. In *Kinsey v. Macur*, 107 Cal. App. 3d 265 (1980), the California Court of Appeal found "the mailing of letters to 'perhaps twenty (people) at most'" sufficient to justify a claim for public disclosure of private facts. *Id.* at 271. The court reasoned that the recipients of the letters "comprised a diverse group of people living in several states and totally unconnected either socially or professionally," and that the group "adequately reflect[ed] 'mass exposure.'" *Id.* at 272. Thus, a claim for public disclosure of private facts is not "one of total secrecy," rather "it is the right to define one's circle of intimacy." *Id.*

Here, Facebook "published private content and information of Plaintiffs and Class Members to unauthorized parties, . . . including millions of app developers." ¶ 522; *see also* ¶ 338 ("[I]t is known that millions of apps had access to users' data prior to Facebook's 2014 platform changes."). Further, Facebook published this information to other third parties, including Facebook's business partners, as well as those who subsequently acquired Plaintiffs' information. Thus, Plaintiffs sufficiently allege public disclosure.

Moreover, Facebook's challenge to this claim, that Plaintiffs "do not specify whether their privacy settings were anything other than 'public,'" should be rejected for the same reasons set forth above in Section II.D.3.

3. Facebook Violated Plaintiffs' Right of Publicity.

First, the Court should not rely on Facebook's argument that Plaintiffs must demonstrate "that the defendant used the plaintiff's identity in a manner related to the plaintiff's 'notoriety.'" *Cf.* MTD 39 (citation omitted). The cases regarding "notoriety" cited by Facebook pertain to a *celebrity's* right to publicity, whereas California law also protects non-celebrity plaintiffs from the appropriation of their name and likeness without regard to notoriety. *See KNB Enters. v.*

Matthews, 78 Cal. App. 4th 362 (2000); *Dora v. Frontline Video, Inc.*, 15 Cal. App. 4th 536, 542 (1993); *cf.* MTD 39 (citing *Newton v. Thomason*, 22 F.3d 1455, 1461 (9th Cir. 1994); *Timed Out, LLC v. Youabian, Inc.*, 229 Cal. App. 4th 1001, 1006 (2014)).

Second, contrary to its claims, Facebook appropriated Plaintiffs' names and likenesses for commercial or other advantage. *Cf.* MTD 39; *see Eastwood v. Superior Court*, 149 Cal. App. 3d 409, 417 (1983). Here, Facebook gained a commercial advantage by making Plaintiffs' personal information—including their names and photographs—available to third parties in exchange for their development and use of Facebook's platform. ¶¶ 119-21. For example, Facebook profited from advertising purchased by Cambridge Analytica, after Facebook allowed Cambridge Analytica to obtain Plaintiffs' personal information. ¶ 374. Similarly, Facebook gained a commercial advantage when it entered into contractual agreements with its business partners, which allowed these partners to obtain users' information, including their names and likenesses. For instance, granting its partners access to Plaintiffs' content and information enabled Facebook to promote and expand its platform across devices and service providers, resulting in an exponential rate of growth and significant commercial benefit to Facebook, as evidenced by the drastic increase in Facebook's average revenue per user over the Class Period. ¶¶ 170, 359, 360, 400-01.

F. Plaintiffs State a Claim for Fraudulent Omission.

Fraudulent omission under California law has five elements: (1) concealing or suppressing a material fact; (2) a duty to disclose the fact; (3) intentionally concealing or suppressing the fact with the intent to defraud; (4) the plaintiff was unaware of the fact and would not have acted as he did if he had known; and (5) due to the concealment or suppression, the plaintiff suffered damage. *In re Yahoo! Inc. Customer Data Sec. Breach Litig.* (“*In re Yahoo! II*”), 313 F. Supp. 3d 1113, 1133 (N.D. Cal. 2018). Facebook's arguments go exclusively to the

first, second, and fifth elements.²³ Plaintiffs allege three fraudulent omissions. All three sets of allegations state a claim.

First, Facebook fraudulently failed to disclose the known risk that third-party app developers would sell or disperse user content and information. ¶ 486. Facebook had a duty to disclose this fact as early as 2011, ¶¶ 322-24, 322 n.121, and certainly by 2014, when Facebook employees learned that Cambridge Analytica was harvesting user data, ¶ 423. Facebook insists that it properly disclosed the fact, MTD 35, but as discussed above, it raises, at most, a question of fact on that point. *See supra* Section II.B.3. Facebook also argues that “there is no duty to disclose a risk of third-party wrongdoing.” MTD 35. That assertion is irrelevant here, because Plaintiffs’ allegations concern Facebook’s own actions. Facebook, not third parties, had the relationship with Plaintiffs that gives rise to the duty. As *In re Yahoo! II* demonstrates, Facebook is not insulated from a fraud claim merely because third parties may exploit Facebook’s own vulnerabilities. 313 F. Supp. 3d at 1133. *Davidson v. City of Westminster*, 32 Cal. 3d 197, 203 (1982), MTD 35, is not to the contrary. *Davidson* considered whether a municipality owed a duty of reasonable care to warn against a stabbing that occurred at a laundromat that was under police surveillance. It did not purport to address a duty to disclose in other contexts. Facebook’s argument that there is no duty to disclose, MTD 34, ignores Plaintiffs allege that the statements made by Facebook executives give rise to a duty to disclose. ¶¶ 345-354.

Second, Facebook fraudulently concealed that it distributes users’ content and information to app developers, as well as its “business partners.” ¶ 496. Facebook had a duty to disclose the true nature of Plaintiffs’ content and information exposure, because it made “affirmative representations that (1) Plaintiffs could control their content and information, and

²³ Plaintiffs satisfy Rule 9(b). *Cf.* MTD 34 (conclusorily stating that Plaintiffs have failed to satisfy the rule). Plaintiffs here provide the same degree of specificity in their claims as the plaintiffs in *Vizio*, by alleging that Facebook (who) failed to disclose the uses of Plaintiffs’ content and information, and that this private information was not secure (what); and that these omissions occurred from 2010 through 2018, while Facebook made statements in the media, on its website, and in its policies that provided a false sense of privacy (when and where) and put Facebook under a duty to disclose. ¶¶ 345-54, 487.

(2) third parties could not access personal data absent users' consent." ¶¶ 227-30, 347, 504.

While Facebook argues that it made sufficient disclosures, Facebook identifies no disclosures at all about giving business partners such as mobile carriers and chip designers access to Plaintiffs' content and information. ¶¶ 112-13.

Third, Facebook fraudulently concealed how users' "content and information was being collected, shared and aggregated to develop digital profiles or dossiers of each user." ¶ 503. Facebook maintains it fully disclosed this fact, but it conflates advertising that Plaintiffs are not challenging, such as routine banner advertisement, with psychographic advertising and advertising that allowed users to be targeted by individual demographic traits (some of them protected by antidiscrimination laws), aided by outside sources of data from data brokers. ¶¶ 366, 371-75, 378-82.

Facebook's contention that Plaintiffs fail to allege damages is unavailing. MTD 36. As Facebook's own authority demonstrates that actions that a plaintiff undertakes—but would not have undertaken had the defendant told the truth—are compensable. *Tenet Healthsystem Desert, Inc. v. Blue Cross of Cal.*, 245 Cal. App. 4th 821, 844 (2016) (hospital treated patients it otherwise would not have if disclosures had been made).

Finally, Judge Chen's ruling in *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051 (N.D. Cal. 2015), which Facebook fails to acknowledge, shows that Plaintiffs have successfully alleged fraudulent omissions. *Carrier IQ* sustained a claim for fraudulent omission under the UCL related to the failure to disclose that smartphone software collected and transferred users' personal data. *Id.* at 1114-15. The claim for fraudulent omission was premised on the defendant's failure to disclose the true nature of its uses of personal information. Here, likewise, Plaintiffs allege that Facebook failed to disclose the ability of third parties to override their privacy settings as well as Facebook's practices allowing Plaintiffs to be targeted by advertising. As in *Carrier IQ*, *In re Yahoo! II*, and *Vizio*, Facebook suppressed the true facts about the actual nature of the technology, and users of the technology unwittingly shared their personal information with third

parties. Had the true facts about the uses of personal information been disclosed and known, users would not have used the technology in the same way, if at all.

G. Facebook Violated the Unfair Competition Law.

1. Plaintiffs Have Standing to Assert UCL Claims

Plaintiffs have standing for purposes of California’s Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, et seq. (“UCL”). They allege that they conveyed their personal content and information to Facebook, that this content and information is of value, and that Facebook has wrongfully monetized and profited from their personal content and information, entitling Plaintiffs to restitution. Entitlement to restitution is sufficient to demonstrate a loss of money or property under the UCL and also satisfies Article III standing. *Anthem II*, 2016 WL 3029783, at *30. In this regard, Facebook’s reliance on *In re Sony Gaming Networks and Customer Data Sec. Breach Litigation*, 903 F. Supp. 2d 942, 963 (S.D. Cal. 2012), is misplaced. In *Sony*, there was no restitution under the UCL because “Sony did not benefit financially from the Data Breach,” whereas here Facebook has profited enormously from its wrongdoing. *Id.* at 970. Also, to the extent Facebook relies on *Sony* for the proposition that Plaintiffs lack UCL standing because there is no “property value in one’s information,” *id.* at 966, this conclusion has been repeatedly rejected. *Anthem I*, 162 F. Supp. 3d at 986.

2. Plaintiffs State a UCL Claim Under the “Unlawful” Prong.

Plaintiffs plead violations of the VPPA and the SCA, and thus have sufficiently pleaded a UCL claim under the “unlawful” prong. *See In re Yahoo! Inc. Customer Data Sec. Breach Litig.* (“*In re Yahoo! I*”), 2017 WL 3727318, at *23 (N.D. Cal. Aug. 30, 2017) (“To the extent that Plaintiffs have sufficiently alleged these stand-alone causes of action, Plaintiffs have also alleged violations of the unlawful prong of the UCL.”).

3. Plaintiffs State a UCL Claim Under the “Fraudulent” Prong.

Plaintiffs allege deceitful conduct and a valid cause of action for a fraudulent omission, which serves as the basis of a UCL claim under the “fraudulent” prong. *Id.* at *30.

4. Plaintiffs State a UCL Claim Under the “Unfair” Prong.

“The ‘unfair’ prong of the UCL creates a cause of action for a business practice that is unfair even if not proscribed by some other law.” *See In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1226 (N.D. Cal. 2014). Here, Plaintiffs allege that Facebook’s actions have violated California’s strong public policy of protecting privacy by exploiting Plaintiffs’ content and information and failing to secure it. ¶ 567. Indeed, Facebook externalizes all of the costs related to protection of personal information, requiring Plaintiffs to take independent action to protect themselves from Facebook’s uses of their private information. ¶¶ 409-16. At this stage, these allegations are sufficient to state a claim under the unfair prong. *See In re Anthem, Inc. Data Breach Litig.* (“*Anthem I*”), 162 F. Supp. 3d 953, 990 (N.D. Cal. 2016); *In re Adobe*, 66 F. Supp. 3d at 1227; *see also In re iPhone Application Litig.*, 844 F. Supp. 2d at 1073 (plaintiffs alleged that the harm from Apple’s tracking of users outweighs its social utility). Facebook’s argument that claims under the “unfair” prong are limited to competition claims, MTD 44, ignores the rulings in *Adobe*, *Anthem I*, and *In re iPhone Application Litigation*.²⁴

5. Plaintiffs Plead Entitlement to UCL Restitution.

Plaintiffs have pleaded two separate theories of restitution under the UCL: (1) payment of out-of-pocket costs for credit monitoring; and (2) Facebook’s exploitation of Plaintiffs’ property interest in their content and information. Allegations of purchase of credit monitoring and identity theft protection alone demonstrate entitlement to restitution under the UCL. *Anthem II*, 2016 WL 3029783, at *32 (allowing plaintiffs to seek restitution “[a]lthough California Plaintiffs might not have paid Defendants directly”). This result is consistent with the California Supreme Court’s holding that economic harm includes circumstances wherein a plaintiff is “required to

²⁴ Facebook cites *Cel-Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.*, 20 Cal. 4th 163, 187 (1999); *Durrell v. Sharp Healthcare*, 183 Cal. App. 4th 1350, 1366 (2010); and *Byars v. SCME Mortgage Bankers, Inc.*, 109 Cal. App. 4th 1134, 1147 (2003), for the proposition that “unfair” under the UCL is limited to harms to competition. MTD 44. None of those cases, however, purport to limit the “unfairness” prong for consumers to antitrust claims, and the requirement that the unfairness prong concern a harm to competition directly applies only “in the context of an unfair competition claim by a competitor.” *Durrell*, 183 Cal. App. 4th at 1364 (emphasis in original).

enter into a transaction, costing money or property, that would otherwise have been unnecessary.” *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 323 (2011).

The UCL also allows Plaintiffs to recover the profits Facebook wrongly reaped from their content and information. Such restitution is authorized when plaintiffs have an ownership interest in a defendant’s profits. *See In re Google Android Consumer Priv. Litig.* (“*Google Android Litig. II*”), 2014 WL 988889, at *7 (N.D. Cal. Mar. 10, 2014) (“Although Plaintiffs do not allege facts that show they paid money directly to Google, the Court cannot conclude that Plaintiffs might not be able to show an ownership interest in at least some of Google’s profits.”). In *Google Android Litigation II*, as here, it was alleged that the defendant collected personal information without the plaintiffs’ consent. Judge White ruled that the plaintiffs could collect as restitution the value of their wrongfully obtained information. *Id.* at *7. The UCL requires this result, because it permits restitution when “a present or future property interest [is] diminished.” *Kwikset*, 51 Cal. 4th at 323.

Facebook incorrectly suggests that Plaintiffs are seeking damages. MTD 44. Plaintiffs, however, do not ask for the recovery of all profits. They seek only those profits Facebook derived directly from its wrongful taking of the content and information in which Plaintiffs had an ownership interest. The California Supreme Court, in the very cases on which Facebook relies, has approved this remedy under the UCL. *See Korea Supply Co. v. Lockheed Martin*, 29 Cal. 4th 1134, 1149 (2003) (citing *Kraus v. Trinity Mgmt. Servs.*, 23 Cal. 4th 116, 126-27 (2000)).

H. Facebook Was Unjustly Enriched Through Its Sale of Access to Plaintiffs’ Content and Information.

Facebook has made billions of dollars by selling access to Plaintiffs’ content and information. “To establish a claim for quantum meruit, the plaintiff must prove that: (1) the plaintiff rendered services to the defendant’s benefit; and (2) the defendant would be unjustly enriched if the plaintiff was not compensated.” *Precision Pay Phones v. Qwest Commc’ns Corp.*, 210 F. Supp. 2d 1106, 1112 (N.D. Cal. 2002). The Complaint alleges both that Plaintiffs rendered services to Facebook’s benefit and that Facebook would be unjustly enriched if

Plaintiffs were not compensated. *See* ¶¶ 3, 109-10, 53, 339, 353-67, 467-68, 478-80, 540, 611-18. These allegations are unchallenged.

1. This Claim Is Not Barred by Facebook’s Agreement with Users.

Facebook argues that this claim is not viable because Plaintiffs assert an express contract. At the motion to dismiss stage, however, it is premature for a court to take a position on whether an action derives solely from any agreement alleged. *Stitt v. Citibank*, 942 F. Supp. 2d 944, 960 (N.D. Cal. 2013) (citing *In re: Countrywide Fin. Corp. Mortg. Mktg. & Sales Practices Litig.*, 601 F. Supp. 2d 1201, 1220-21 (S.D. Cal. 2009)); *see also Ellis v. J.P. Morgan Chase & Co.*, 950 F. Supp. 2d 1062, 1091 (N.D. Cal. 2013). “[M]otions to dismiss claims for unjust enrichment are disfavored ‘because it is difficult to determine the validity or scope of the contract at the pleading stage.’” *Circle Click Media LLC v. Regus Mgmt. Grp. LLC*, 2013 WL 57861, at *13 (N.D. Cal. Jan. 3, 2013) (applying New York law but noting similarity to California law). Under California law, “quasi-contract actions may be utilized to prevent unjust enrichment regarding disputes between contracting parties that are related to, but outside the scope of, the parties’ contract.” *Raisin Bargaining Ass’n v. Hartford Cas. Ins. Co.*, 2010 WL 3783871, at *3 (E.D. Cal. Sept. 27, 2010); *see also Aerojet-Gen. Corp. v. Transport Indem. Co.*, 17 Cal. 4th 38, 69 (1997) (allowing unjust enrichment to party to an insurance contract).

Moreover, Facebook’s sale of user data to third-party business partners was not covered by the SRR. Because no adequate legal remedy is available under any applicable contract for Facebook’s unauthorized sale of users’ content and information to third-party business partners, Plaintiffs may bring a claim in quasi-contract on behalf of themselves and their fellow putative Class Members to pursue restitution based on Facebook’s unjust enrichment. *Countrywide*, 601 F. Supp. 2d at 1220-21 (rejecting defendants’ arguments for dismissal of an unjust enrichment claim, holding that “[a]lthough there are contracts at issue in this case, none appears to provide for the specific recovery sought by Plaintiffs’ unjust enrichment claim”); *Bertino & Assocs., Inc. v. R L Young, Inc.*, 2013 WL 3949028, at *6 (D.N.J. Aug. 1, 2013) (applying California law)

(“[T]he facts pled do raise some question as to whether the work was within the scope of the Agreement.”).

2. Restitution Is the Appropriate Remedy in Quasi-Contract.

Plaintiffs allege that exploitation of their content and information conferred a benefit to Facebook. *See Astiana v. Hain Celestial Grp., Inc.*, 783 F.3d 753, 762 (9th Cir. 2015) (“The return of that benefit is the remedy ‘typically sought in a quasi-contract cause of action.’”). Allegations that private information about a person has been monetized without consent makes restitution an appropriate remedy. *Moeller v. Am. Media, Inc.*, 235 F. Supp. 3d 868, 873 (E.D. Mich. 2017) (magazine subscribers had standing against media company for “disclosing personal-reading information to data-mining companies and third-party database cooperatives”).

Under quasi-contract, “a plaintiff who has rendered services benefitting the defendant may recover the reasonable value of those services when necessary to prevent unjust enrichment of the defendant.” *In re De Laurentiis Entm’t Grp.*, 963 F.2d 1269, 1272 (9th Cir. 1992) (citing B. Witkin, Summary of California Law: Contracts § 91 (1987) (“Witkin”)). Facebook gave third parties unauthorized access to its users’ personal information to obtain advertising revenue for its own financial benefit.

Unfortunately, the Cambridge Analytica scandal represents only the tip of the iceberg with respect to Facebook’s willful pursuit of generating revenue at the expense of its users. Facebook’s sale of its users’ information to third parties reflects a calculated business decision designed to benefit Facebook at its users’ expense. ¶¶ 8, 225, 312, 322-26, 335-37, 352, 374, 380, 406, 412-14, 425, 431, 487-90, 550-51. Under this cause of action, Plaintiffs seek compensation for the costs Facebook externalized on to them, and recovery of Facebook’s ill-gotten gains.

I. Plaintiffs State a Claim for Negligence and Gross Negligence.

Facebook’s principal argument against Plaintiffs’ negligence-based claim is that it owed them no duty of care.²⁵ Facebook is incorrect.

California has long recognized a duty of care owed by the defendant to the plaintiff from transactions involving third parties, even if the plaintiff suffers only economic loss. *See, e.g., In re Yahoo! II*, 313 F. Supp. 3d at 1132-33. Here, Plaintiffs allege they “entrusted with . . . their content and information” to Facebook, “which provided an independent duty of care.” ¶ 548. Plaintiffs do *not* ground that duty in the contracts between Facebook and Plaintiffs. Instead, they ground their claim in a duty independent of any contractual duty. *Cf.* MTD 40.

To determine whether Facebook owes a duty for Plaintiffs’ economic losses, California law looks to the six *J’Aire* factors. *See In re Yahoo! II*, 313 F. Supp. 3d at 1132 (citing *J’Aire Corp. v. Gregory*, 24 Cal. 3d 799, 804 (1979)). In applying the first *J’Aire* factor, the extent to which the transaction was intended to affect the plaintiff, California law examines the “primary purpose” of the transaction. *In re Yahoo! II*, 313 F. Supp. 3d at 1129. Here, the primary purpose of the transaction between Facebook and Global Science Research Limited (“GSR”) was to provide access to the Plaintiffs’ content and information. *See, e.g.,* ¶¶ 113, 135, 144-45. “The impact on plaintiffs cannot be characterized as ‘collateral’” to the transaction. *Centinela Freeman Emergency Med. Assocs. v. Health Net of Cal., Inc.*, 1 Cal. 5th 994, 1015 (2016). Rather, the transaction “was necessarily intended to have an effect on plaintiffs.” *Id.* at 1014.

The second factor, foreseeability of harm, favors Plaintiffs. Facebook was well aware as early as 2011 and 2012 that users’ content and information was vulnerable to misuse by app developers using Graph API v.1.0. *See* ¶¶ 322-24, 322 n.121.

The third factor, the degree of certainty that Plaintiffs suffered injury, supports Plaintiffs. As explained above, Plaintiffs have alleged in detail why they have suffered economic injury. *See supra* Section II.A.3.

²⁵ Facebook also argues that Plaintiffs’ claim is defeated by their consent, by the SRR’s exculpatory clause, and by a lack of damages. These arguments are incorrect for reasons already stated above. *See supra* Section II.B.

Fourth is the closeness of the connection between the defendant's conduct and the injury suffered. This factor is satisfied because Facebook's transactions with GSR and other app developers "brought . . . plaintiffs[] into a position of risk," and without those transactions, the app developers "would have had no impact on plaintiffs." *Centinela*, 1 Cal. 5th at 1016. "Therefore, if, as plaintiffs allege," Facebook "knew or should have known" when contracting with the app developers that failure to take reasonable precautions would allow the app developers to misuse plaintiffs' content and information, then Facebook's conduct "is closely connected to plaintiffs' losses." *Id.*

Fifth is the moral blame attaching to the defendant's conduct, which here is substantial. Even after Facebook knew that users' content and information was vulnerable to misuse by app developers, Facebook continued to violate the FTC Consent Decree by taking no meaningful steps to protect them. ¶¶ 322-24 & n.121. This "lack of diligence" is "particularly blameworthy since it continued after the probability of damage was drawn directly to [Facebook's] attention." *J'Aire*, 24 Cal. 3d at 805. Not until April 2018—at least two years after it became aware—did Facebook notify affected users that Cambridge Analytica had accessed their data. *See* ¶¶ 142, 154. Relevant, too, was Plaintiffs' "understanding that Facebook would take appropriate measures" to protect their content and information, and the billions of dollars of revenue that Facebook has generated precisely because of this understanding. ¶¶ 548-49; *see Beacon Residential Cmty. Ass'n v. Skidmore, Owings & Merrill LLP*, 59 Cal. 4th 568, 586 (2014) (moral blame attached to defendants' conduct due to their "unique and well-compensated role" and "their awareness" that plaintiffs were relying on them).

Last is the "policy of preventing future harm," which "is ordinarily served, in tort law, by imposing the costs of negligent conduct upon those responsible," *Cabral v. Ralphs Grocery Co.*, 51 Cal. 4th 764, 781 (2011). That policy is furthered by imposing those costs on Facebook, particularly because it was Facebook that is best positioned to avoid or spread them. *See Beacon Residential*, 59 Cal. 4th at 585. As the *J'Aire* factors are met here, Facebook's argument that the economic loss rule bars their claims lacks merit.

In a similar case, Judge Koh determined that the *J'Aire* factors favored recognition of a duty of care. In *In re Yahoo! II*, email users—like the Facebook users here—turned over their personal information “with the understanding that Defendants would adequately protect” it and inform the plaintiffs of breaches. There, as here, “Defendants knew their data security was inadequate,” but did not take steps to correct it or to “promptly notify” the plaintiffs that their data had been compromised. 313 F. Supp. 3d at 1132. Just as Yahoo! was in that case, Facebook is under a duty of care here. *Id.* at 1132-33.

Citing inapposite cases, Facebook maintains that it owes no duty of care to Plaintiffs. *See* MTD 40 (citing *Google Android Litig. I*, 2013 WL 1283236; *Pirozzi v. Apple Inc.*, 913 F. Supp. 2d 840 (N.D. Cal. 2012); *In re iPhone Application Litig.*, 2011 WL 4403963). In each case Facebook cites, purchasers of smartphones asserted that the phone maker owed them a duty to prevent applications available at Apple’s App Store or Google’s Android Market from wrongly taking the purchasers’ personal information. This case involves dispositively different facts. Plaintiffs’ negligence claims do not rely simply Facebook’s status as developer of a platform. Here, moreover, Facebook knew for years that its users’ content was vulnerable, and took no steps to remedy the problem. ¶¶ 322-24, 322 n.121; *see In re Yahoo! II*, 313 F. Supp. 3d at 1131-32 (holding that negligence claim satisfied *J'Aire* because complaint alleged that Yahoo knew of specific security risks and took no action).²⁶

²⁶ Facebook’s authorities generally deal with manufacturers and retail customers, or do not address a special relationship, and thus are inapposite. MTD 40-41; *In re: Lenovo Adware Litig.*, 2016 WL 6277245, at *9 (N.D. Cal., Oct. 27, 2016) (laptop manufacturer); *Greystone Homes, Inc. v. Midtec, Inc.*, 168 Cal. App. 4th 1194, 1231 (2008) (plumbing fitting manufacturer); *Ott v. Alfa-Laval Agri, Inc.*, 31 Cal. App. 4th 1439, 1456 (1995) (mechanical milking system); *Platte Anchor Bolt, Inc. v. IHI, Inc.*, 352 F. Supp. 2d 1048, 1055 (N.D. Cal. 2004) (supplier of bolts to subcontractor); *Stewart v. Electrolux Home Prods., Inc.*, 304 F. Supp. 3d 894, 903 (E.D. Cal. 2018) (oven manufacturer). *In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089 (N.D. Cal. 2013) does not address the *J'Aire* factors, and Plaintiffs plead the “something more” associated with misappropriation of their content and information discussed there.

J. In the Alternative to Quasi-Contract, Facebook Breached the Terms of the SRR With Users.

1. Plaintiffs Have Standing to Pursue a Breach of Contract Claim.

Plaintiffs have standing under Article III to pursue a breach of contract claim even if they have not suffered economic harm. This is true for two reasons. First, a breach of a contractual promise, even without more, “has traditionally been regarded as providing a basis for a lawsuit in English [and] American courts.” *Spokeo*, 136 S. Ct. at 1549. The California Civil Code, enacted in 1872, provides that even if a breach “has caused no appreciable detriment,” the party affected “may yet recover nominal damages.” Cal. Civ. Code § 3360. This rule has been reaffirmed by the courts. *See, e.g., Sweet v. Johnson*, 169 Cal. App. 2d 630 (1959); *see also* Witkin, *supra*, § 903. Second, the California Legislature’s judgment that a contractual breach is actionable by itself is owed deference. *See Spokeo*, 136 S. Ct. at 1549 (legislative judgment “instructive and important”); *see also Patel v. Facebook Inc.*, 290 F. Supp. 3d 948, 953 (N.D. Cal. 2018) (deferring to state legislature’s view of what constitutes an actionable injury). For these reasons, a breach of an enforceable contractual promise, even without other damage, constitutes an injury in fact. *See In re Facebook Privacy Litig.*, 192 F. Supp. 3d 1053, 1060-62 (N.D. Cal. 2016). *Aguilera*, 223 F.3d 1010, cited by Defendants, does not hold otherwise. There, the Ninth Circuit held merely that a breach of contract claim “depends on a showing that they suffered legally cognizable harm” as of the date of breach—which Plaintiffs have shown. *Id.* at 1015 (declining to recognize fear of future layoff as actionable injury).

2. Facebook Breached Its Promise Not to Share Content and Information With Third Parties.

In the SRR, Facebook promised that it would “not share your content and information with advertisers without your consent.” ¶¶ 228-33. Despite that promise, Facebook granted third-party app developers and business partners access to users’ information.²⁷ Facebook maintains

²⁷ Facebook attached 49 documents to the Declaration of Michael Duffey in Support of Facebook, Inc.’s Motion to Dismiss Plaintiffs’ Consolidated Complaint (“Duffey Declaration”), ECF No. 187, that was attached to the Request for Judicial Notice in Support of Defendant Facebook, Inc.’s Motion to Dismiss Plaintiffs’ Consolidated Complaint (“Request”), ECF No.

these third parties are not advertisers, MTD 41-42, but that is simply false. Facebook’s business partners, like Amazon, Qualcomm, and Samsung, advertised on Facebook.

Likewise, Facebook violated its contractual agreement that users “own[ed] all of the content and information [they] post[ed] on Facebook, and . . . c[ould] control how it is shared.” ¶¶ 219-22. By acknowledging that users owned their content and information, Facebook guaranteed it would only disclose users’ content and information to third parties when the SRR explicitly allowed for sharing. That is the nature of ownership: “[t]he ownership of a thing is the right of one or more persons to possess and use it to the exclusion of others.” Cal. Civ. Code § 654. Yet the SRR explicitly allowed sharing with apps *only* if users had added the app to their Facebook account. Indeed, earlier versions of the SRR stated that a Facebook user’s content and information would be shared with an app “[w]hen” the user “add[ed]” the application. ¶¶ 220-21. Also, while later versions say that the user of an app may permit the app to access the content and information of that user’s friends, that provision did not bind the user’s friends. A contract cannot bind third parties without their consent. *See, e.g., Cty. of Contra Costa v. Kaiser Found. Health Plan, Inc.*, 47 Cal. App. 4th 237, 242-43 (1996) (stating that contracts cannot bind nonsignatories absent preexisting relationship or third-party beneficiary status).

For that reason, by sharing users’ content and information with the MyDigitalLife and other apps, Facebook breached the SRR provision that users owned all of the content and information they posted on Facebook and could control how it is shared. *See, e.g.*, ¶¶ 8, 135, 138, 145-48, 225, 338. Even if the users of those applications had consented, the friends had not. Hence, the apps’ ability to access the friends’ content and information breached the SRR as to each friend.

185, describing them as “contractual documents.” Plaintiffs oppose Facebook’s Request for the reasons set forth in their Opposition. These include that they are not contracts; that the hard copy documents do not represent how policies appeared onscreen; or address how they were accessible to users. Furthermore, the Request does not identify the website where these documents were available or for what period of time. For the reasons set forth in Plaintiffs’ Opposition, the Request should be denied.

3. Plaintiffs Have Suffered Damages.

Facebook incorrectly claims that Plaintiffs have not suffered damages from its breach of contract. Plaintiffs contracted to engage on a social platform protected by their own privacy settings. They did not receive that service—they received a less valuable one where many of their privacy settings were meaningless. Users must now accept less privacy than they were promised when they signed on—which is not what they contracted for—or reduce their participation on the site to protect their privacy. ¶ 416; *see Fraley*, 830 F. Supp. 2d at 799 (opportunity costs are economic losses); *see also Hinojos v. Kohl's Corp.*, 718 F.3d 1098, 1108 (9th Cir. 2013) (noting that “damage” includes opportunity costs and transaction costs).

K. Facebook Breached Its Implied Covenant of Good Faith and Fair Dealing with Users.

“[C]ourts routinely allow plaintiffs to plead both express contract and implied contract theories, as long as those theories are clearly pled in the alternative.” *In re Yahoo! I*, 2017 WL 3727318, at *47. Plaintiffs have done exactly that in alleging that, even if Facebook did “not technically transgress[] the express covenants” in their contract with users, Facebook sought to avoid its obligations and deprive Plaintiffs of the benefits of the Terms of Service. ¶ 597; *see Woods v. Google Inc.*, 2011 WL 3501403, at *6 (N.D. Cal. Aug. 10, 2011) (“Woods alleges that irrespective of whether it breached its contractual obligations directly, Google sought to avoid its obligations and deprive Woods and other advertisers of the benefits of the Agreement.”). Moreover, Plaintiffs adequately allege that Facebook deprived them of a benefit to which they were entitled under the contract. *See* ¶¶ 598-608; *see In re Yahoo! I*, 2017 WL 3727318, at *49 (finding that “Plaintiffs have alleged that [Yahoo!] engaged in bad faith by failing to employ minimal reasonable safeguards to protect users’ PII in violation of [its] contractual duties”).

L. All of Plaintiffs’ Claims Are Timely.

Facebook argues certain claims are time-barred, citing to a single 2015 article in *The Guardian*, a U.K. publication. MTD 27-29.²⁸ But the 2015 article in *The Guardian* did not put

²⁸ As set forth in the Opposition to Facebook’s Request for Judicial Notice, Plaintiffs object to judicial notice of *The Guardian* article on grounds other than the existence of the article.

users on notice about the conduct that is the subject of this lawsuit: Facebook allowed friends to overrule users' privacy settings so that it could disseminate user content and information to its business partners and app developers. The article places the blame at the feet of Cambridge Analytica, not Facebook. Users, particularly U.S. users who had no dealings with Cambridge Analytica had no reason to suspect they were affected, especially when Facebook did not tell them. Nor did the article disclose that Facebook's widespread dissemination of private content and information was routine. Facebook also makes no showing that the article was widely circulated sufficient to give proper notice to Plaintiffs. *See, e.g., Eidson v. Medtronic, Inc.*, 40 F. Supp. 3d 1202, 1221 (N.D. Cal. 2014) (collecting cases rejecting defendants' arguments that publicity gave rise to constructive knowledge by plaintiffs).

The claim that users should have investigated is outrageous and turns Facebook's notice obligations on their head. Facebook was required under the terms of the FTC Consent Decree to notify users if their content was improperly accessed. But Facebook did not notify users that Cambridge Analytica obtained their data until 2018. ¶¶ 150-52. Facebook's limitations argument is further undermined by its admission that it "didn't take a broad enough view of our responsibility, and that was a big mistake." ¶ 355; *see also* ¶ 356 (admitting Facebook failed to keep users informed about "the choices they have over their data").

In fact, Facebook repeatedly assured users that their data was secure. ¶ 352. In 2011, Facebook entered into its Consent Decree with the FTC, legally obligating itself to "obtain the user's affirmative express consent" prior to "sharing of a user's nonpublic user information by [Facebook] with any third party which materially exceeds the restrictions imposed by a user's privacy settings." ¶ 298. Each quarter, PricewaterhouseCoopers certified that Facebook was in compliance with the Consent Decree. ¶ 338. Until 2018, Facebook "denied that Cambridge Analytica or any of its associated companies had 'Facebook user data'" and stated it had "no insight on' how Cambridge Analytica may have gathered data from users on Facebook." ¶ 428. Facebook also failed to correct denials by Cambridge Analytica's CEO in testimony before the British Parliament that Cambridge Analytica used Facebook content and information. ¶¶ 429-30.

“If a defendant takes active steps to conceal its misdeed, the statute of limitation is tolled until the plaintiff discovers the claim or would have through ‘the exercise of reasonable diligence.’” *ShopKo Stores Operating Co. v. Balboa Capital Corp.*, 2017 WL 3579879, at *5 (C.D. Cal. July 13, 2017) (citation omitted). Facebook cannot now argue that Plaintiffs should have known it was not telling the truth. *See, e.g., Vucinich v. Paine, Webber, Jackson & Curtis, Inc.*, 739 F.2d 1434, 1436-37 (9th Cir. 1984) (whether defendant’s “reassuring statements” to plaintiff “reasonably affected” when plaintiff was put on notice was “a disputed question of fact”).

Given Facebook’s failure to notify Plaintiffs, despite that it was legally required to do so, and Facebook’s other acts to conceal the truth, Plaintiffs could not have learned of the true facts through a reasonable investigation where even the FTC could not. Facebook alone knew who was affected and did not tell its users. Because Plaintiffs were not able to discover whether they were injured, they would not have discovered the relevant facts, *Merck & Co. v. Reynolds*, 559 U.S. 633, 653 (2010), or gained “knowledge of the harm.” *Jolly v. Eli Lilly & Co.*, 44 Cal. 3d 1103, 1112 (1988). Accordingly, *The Guardian* article did not begin the limitations period as a matter of California or federal law. *Merck*, 559 U.S. at 651, 653 (“[W]here the facts would lead a reasonably diligent plaintiff to investigate further . . . the limitations period does not begin to run.”); *see Fox v. Ethicon Endo-Surgery, Inc.*, 35 Cal. 4th 797, 808-09 (2005) (“[T]he statute of limitations begins to run on that cause of action when the investigation would have brought such information to light.”).

M. Plaintiffs’ Non-California Claims Should Be Dismissed Without Prejudice.

Facebook argues for dismissal of Plaintiffs’ non-California state statutory causes of action because “the parties agree that California law applies.” MTD 45. However, subsequent to the filing of Facebook’s motion, the Court entered Pretrial Order No. 12, which provides that all of Plaintiffs’ claims “that are not included in the twelve prioritized claims in the Consolidated Complaint”—including all non-California state statutory causes of action—are to be stayed pending resolution of the motion to dismiss. ECF No. 190 at 1; *see also* ECF No. 152-2. For this reason, Facebook’s motion to dismiss these claims should be denied.

III. IN THE ALTERNATIVE, PLAINTIFFS SEEK LEAVE TO AMEND

Plaintiffs have stated claims for each of the twelve prioritized causes of action identified in the Complaint. However, in the event the Court finds Plaintiffs have not pleaded facts sufficient to establish any of these claims, Plaintiffs respectfully seek leave to amend. Under Rule 15(a), leave to amend “shall be freely given when justice so requires,” while bearing in mind “the underlying purpose of Rule 15 . . . is to facilitate decision on the merits, rather than on the pleadings or technicalities.” *Lopez v. Smith*, 203 F.3d 1122, 1140 (9th Cir. 2000). Significant developments have occurred since the filing of the Complaint, and investigations into Facebook’s data practices are ongoing. Examples of recent articles bearing on questions of injury, harm, and Facebook’s gross negligence and deceit are attached to the Weaver Declaration submitted herewith. *See* Weaver Declaration ¶¶ 4-6, Exs. 3-4. Moreover, Facebook has resisted all meaningful discovery, refusing to produce any discovery whatsoever relating to its agreements with business partners, notwithstanding it has produced numerous materials in other litigation and proceedings.²⁹ *See* Weaver Declaration ¶ 7. Plaintiffs expect that ongoing investigations will continue to reveal facts bearing on these claims, and would therefore seek leave to amend them should the Court not uphold them.

IV. CONCLUSION

For the reasons set forth above, Plaintiffs ask that the Motion to Dismiss be denied in its entirety.

²⁹ Notably, of the 49 documents Facebook attached to its Duffey Declaration, Facebook produced only 11 of them to Plaintiffs.

Dated: November 30, 2018

Respectfully submitted,

KELLER ROHRBACK L.L.P.

BLEICHMAR FONTI & AULD LLP

By: /s/ Derek W. Loeser
Derek W. Loeser

By: /s/ Lesley E. Weaver
Lesley E. Weaver

Derek W. Loeser (admitted *pro hac vice*)
Lynn Lincoln Sarko (admitted *pro hac vice*)
Gretchen Freeman Cappio (admitted *pro hac vice*)
Cari Campen Laufenberg (admitted *pro hac vice*)
1201 Third Avenue, Suite 3200
Seattle, WA 98101
Tel.: (206) 623-1900
Fax: (206) 623-3384
dloeser@kellerrohrback.com
lsarko@kellerrohrback.com
gcappio@kellerrohrback.com
claufenberg@kellerrohrback.com

Lesley E. Weaver (SBN 191305)
Matthew S. Weiler (SBN 236052)
Anne Davis (SBN 267909)
Emily C. Aldridge (SBN 299236)
555 12th Street, Suite 1600
Oakland, CA 94607
Tel.: (415) 445-4003
Fax: (415) 445-4020
lweaver@bfalaw.com
mweiler@bfalaw.com
adavis@bfalaw.com
ealdridge@bfalaw.com

Christopher Springer (SBN 291180)
801 Garden Street, Suite 301
Santa Barbara, CA 93101
Tel.: (805) 456-1496
Fax: (805) 456-1497
cspringer@kellerrohrback.com

Plaintiffs' Co-Lead Counsel

ATTESTATION PURSUANT TO CIVIL LOCAL RULE 5-1(i)(3)

I, Derek W. Loeser, attest that concurrence in the filing of this document has been obtained from the other signatory. I declare under penalty of perjury that the foregoing is true and correct.

Executed this 30th day of November, 2018, at Seattle, Washington.

/s/ Derek W. Loeser

Derek W. Loeser

CERTIFICATE OF SERVICE

I, Derek W. Loeser, hereby certify that on November 30, 2018, I electronically filed the foregoing with the Clerk of the United States District Court for the Northern District of California using the CM/ECF system, which shall send electronic notification to all counsel of record.

/s/ Derek W. Loeser

Derek W. Loeser